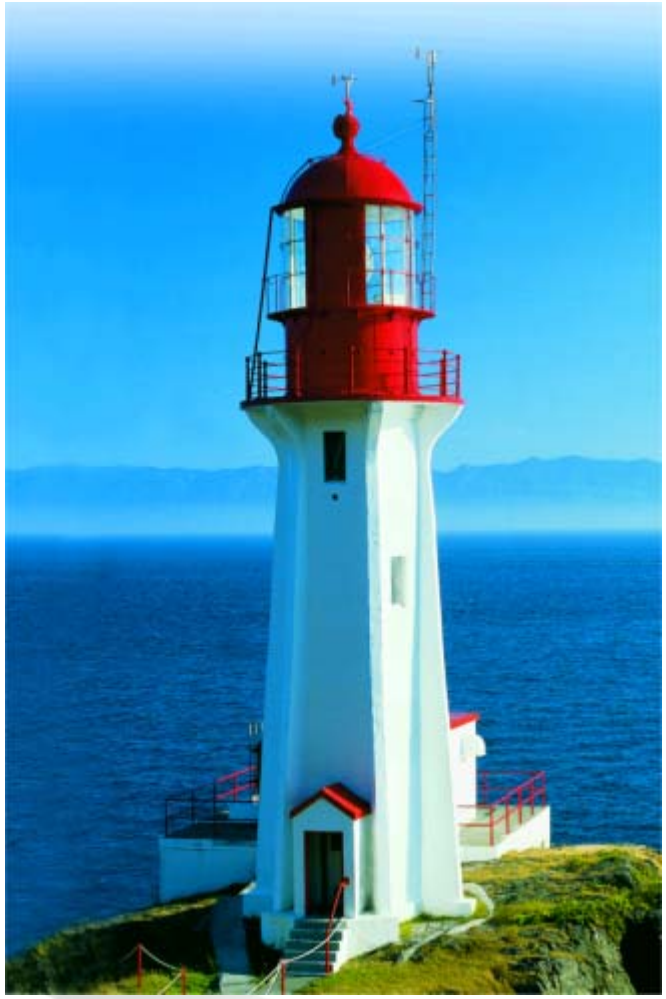


Die Umsetzung des IT-Sicherheitsgesetzes bei den privaten Banken in Deutschland

Jana Ehlers

SRC Security Research & Consulting GmbH

SRC
Security Research & Consulting GmbH

- Gegründet 2000
- knapp 90 Mitarbeiter
- Firmensitz: Bonn und Wiesbaden

Gesellschafter:
Kreditwirtschaftliche Verlage

- Bank-Verlag, Köln
- DG Verlag, Wiesbaden
- DSV, Stuttgart
- VÖB-ZVD, Bonn

Thema: **Sichere Systeme**

- Konzeption, Spezifikation, Entwicklung
- Evaluierung/Begutachtung/Testung/Auditierung
- Beratung, Schulungen und Projektmanagement

Agenda

- Überblick über den Finanzsektor in Deutschland
- Anforderungen des IT-SiG an den Finanzsektor
- Identifikation betroffener Betreiber
- Entwicklung eines Branchenstandards durch die privaten Banken

Überblick über den

FINANZSEKTOR IN DEUTSCHLAND

Finanzsektor in Deutschland

öffentlich

genossen-
schaftlich

privat

bankenverband

Die Deutsche
Kreditwirtschaft

Bundesverband deutscher Banken

- **Spitzenverband der Privatbanken**
- **über 200 private Kreditinstitute**

  z.B. Deutsche Bank, Commerzbank, Hypo-Vereinsbank, Deutsche Postbank, ING-DiBa, …

  und 11 Landesverbände

ANFORDERUNGEN DES IT-SIG

an den Finanzsektor

IT-SiG und BSIG
Anwendungsbereich im Finanzsektor

§ 2 Begriffsbestimmungen

(10) 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.

§ 8c Anwendungsbereich

(1) Die §§ 8a und 8b sind nicht anzuwenden auf Kleinstunternehmen im Sinne der Empfehlung 2003/361/EC der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (ABl. L 124 vom 20.5.2003, S. 36). Artikel 3 Absatz 4 der Empfehlung ist nicht anzuwenden.

IT-SiG und BSIG
Anwendungsbereich im Finanzsektor

Wer gehört im Finanzsektor zu den Betreibern Kritischer Infrastrukturen?

IT-SiG und BSIG
Anforderungen an Maßnahmen

§ 8a Sicherheit in der Informationstechnik Kritischer Infrastrukturen

(1) 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.

(2) Betreiber Kritischer Infrastrukturen und ihre Branchenverbände können branchenspezifische Sicherheitsstandards zur Gewährleistung der Anforderungen nach Absatz 1 vorschlagen. Das Bundesamt stellt auf Antrag fest, ob diese geeignet sind, die Anforderungen nach Absatz 1 zu gewährleisten. Die Feststellung erfolgt

1. im Benehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe,
2. im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde.

(3) 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 eine Aufstellung der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel. Das Bundesamt kann bei Sicherheitsmängeln verlangen:

1. die Übermittlung der gesamten Audit-, Prüfungs- oder Zertifizierungsergebnisse und
2. im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der Sicherheitsmängel.

(4) Das Bundesamt kann zur Ausgestaltung des Verfahrens der Sicherheitsaudits, Prüfungen und Zertifizierungen nach Absatz 3 Anforderungen an die Art und Weise der Durchführung, an die hierüber auszustellenden Nachweise sowie fachliche und organisatorische Anforderungen an die prüfende Stelle nach Anhörung von Vertretern der betroffenen Betreiber und der betroffenen Wirtschaftsverbände festlegen.

IT-SiG und BSIG
Anforderungen an Maßnahmen

Was sind angemessene organisatorische und technische Vorkehrungen?

Wie kann ein Nachweis darüber aussehen?

IT-SiG und BSIG
Meldungen von Vorfällen

§ 8b Zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen

(4) Betreiber Kritischer Infrastrukturen haben erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen

1. führen können oder
2. geführt haben,

über die Kontaktstelle unverzüglich an das Bundesamt zu melden. Die Meldung muss Angaben zu der Störung sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik, der Art der betroffenen Einrichtung oder Anlage sowie zur Branche des Betreibers enthalten. Die Nennung des Betreibers ist nur dann erforderlich, wenn die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt hat.

(5) Zusätzlich zu ihrer Kontaktstelle nach Absatz 3 können Betreiber Kritischer Infrastrukturen, die dem gleichen Sektor angehören, eine gemeinsame übergeordnete Ansprechstelle benennen.

IT-SiG und BSIG
Meldungen von Vorfällen

Welche Störungen müssen gemeldet werden?

Wie können Störungen gemeldet werden?

IT-SiG und BSIG
Folgerungen für Privatbanken

Es sind noch nicht definiert:

- **Betroffene Betreiber** → **Sektorstudie**
- **Angemessene Vorkehrungen**
- **Nachweis der Vorkehrungen** → **Branchenstandard**
- **Meldungen**

IDENTIFIKATION BETROFFENER BETREIBER

für den Finanzsektor

Betroffene Betreiber
Grundlage der Definition

- **Rechtsverordnung**
- **Sektorstudien als Grundlage**
  - durch BSI in Auftrag gegeben
  - für verschiedene Sektoren

Betroffene Betreiber
Relevante Dienstleistungen

Was könnte im Finanzsektor „kritisch“ sein?

Ressorts	BaFin	BSI-Sektorstudie*
Zahlungsverkehr • Kartenzahlung • Überweisung • E-Geld	Zahlungsverkehr • Kartenzahlung • Online-Banking (einschl. Mobile-Banking)	Zahlungsverkehr • Kartenzahlungen • Abwicklung bargeldlosen Zahlungsverkehrs
Bargeldversorgung	Bargeldversorgung	Bargeldversorgung
Wertpapier- und Derivatehandel		Wertpapier- und Derivatehandel
Kreditvergabe		
Geld- und Devisenhandel		
Versicherungsleistungen		
	Dienstleistungen, bei denen Vorfälle zu einer Verletzung der Vertraulichkeit analog § 42a BDSG oder zu signifikanten Reputationsschäden führen können oder die vom Institut als Notfall gewertet werden	

* unter Vorbehalt

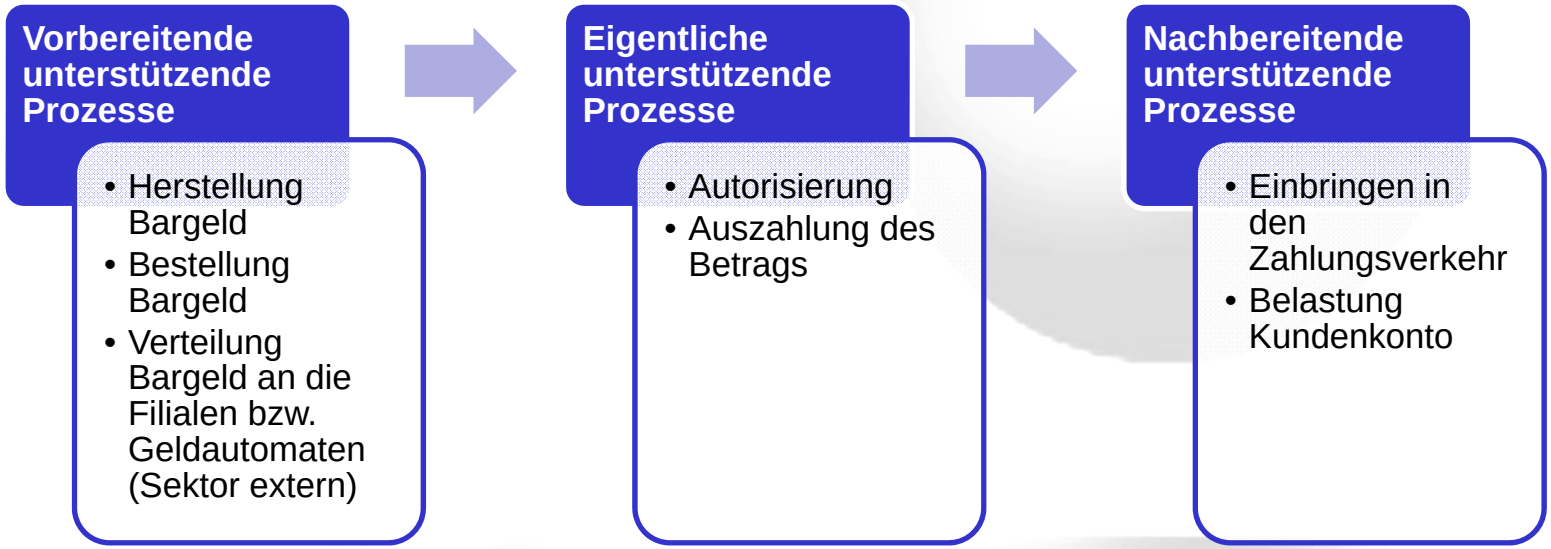
Betroffene Betreiber
Relevante Dienstleister

SRC security consulting

Wer erbringt diese Dienstleistungen?

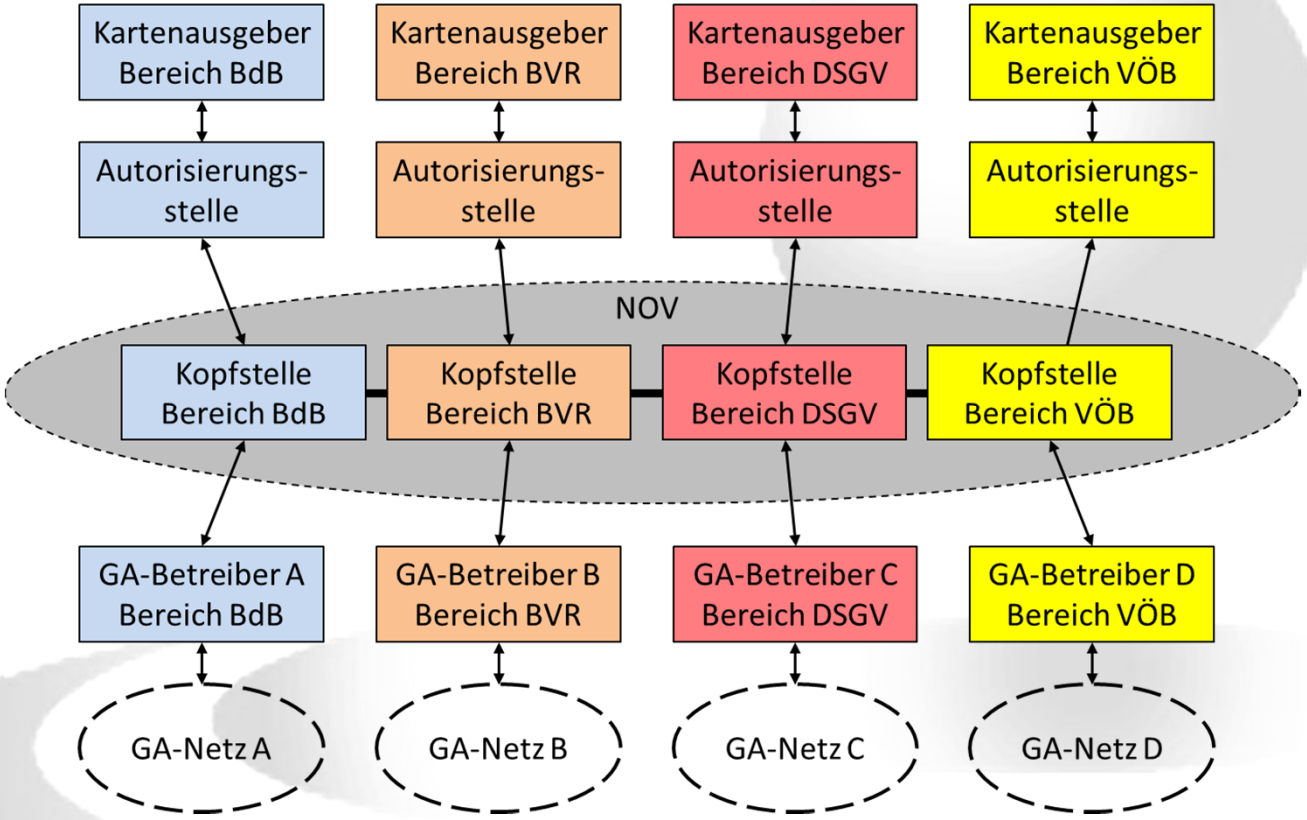
Betroffene Betreiber
Relevante Dienstleister

Beispiel Bargeldversorgung



Betroffene Betreiber
Relevante Dienstleister

Beispiel Bargeldversorgung



ENTWICKLUNG EINES BRANCHENSTANDARDS

durch die privaten Banken

Branchenstandard
Ziele

Definition von

- angemessene Vorkehrungen
- Nachweis der Vorkehrungen
- Meldungen (was und wie)

für die Privatbanken

Branchenstandard
Anforderungen des BSI

BSI hat herausgegeben:

- **Anforderungskatalog-Entwurf für branchenspezifische Sicherheitsstandards**
- **Abgleich zwischen den Anforderungen aus dem Gesetzestext und div. Standards**

Branchenstandard
Anforderungskatalog-Entwurf

Branchenstandardanforderung	
Anforderungen aus dem Gesetzestext • Festlegung von Schutzzielen • Ableitung der Schutzziele aus KRITIS-Forderungen • Prüfschema	• Standard adressiert Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der IT-Systeme, IT-Komponenten und IT-Prozesse • IT-Schutzziele werden konsequent aus den übergeordneten Schutzzielen der kDL abgeleitet und in allen Themenbereichen konsequent berücksichtigt • Standard referenziert geeignetes Schema (inkl. fachliche und organisatorische Anforderungen an die prüfende Stelle, Umfang und Tiefe der Prüfung, Prüfprozess).
Anforderungen an inhaltliche Ausrichtung	
Abstraktionsgrad • Abzudeckende Themen und Detailtiefe	• Im B3S werden alle abzudeckenden Themen adressiert und zwar mindestens in einer Detailtiefe, die in etwa Anhang A der ISO27001 bzw. ISO27002 entspricht.
Anforderungen an das Risikomanagement	
Anforderungen an im Standard abzudeckende Themen • ISMS • Branchenspezifische Technik	• Standard thematisiert ISMS • Standard geht auf Besonderheiten der branchenspezifischen Technik ein (z.B. Sicherheits-Schwächen/-Stärken verwendeter Geräte/Software/Protokolle
Anforderungen an Maßnahmen, die folgenden Bedrohungen und Schwachstellen begegnen: …	
Wirtschaftlichkeit und Skalierbarkeit	
Formale Anforderung	
Vorgabe zur Übermittlung	

Branchenstandard
Abgleich Anforderungen – Standards

Branchenstandard-anforderung / ISO-Standard	27001	27002	27015
Anforderungen aus dem Gesetzestext			
• Festlegung von Schutzzielen	✓✓	✓✓	✗
• Ableitung der Schutzziele aus KRITIS-Forderungen	✗	✗	✗
• Prüfschema	✓	✗	✗
Anforderungen an inhaltliche Ausrichtung			
Abstraktionsgrad			
• Abzudeckende Themen und Detailtiefe	✗	✓	✓✓
Anforderungen an das Risikomanagement			
Anforderungen an im Standard abzudeckende Themen			
• ISMS	✓✓	✓✓	✓✓
• Branchenspezifische Technik	✗	✗	✓✓
Anforderungen an Maßnahmen, die folgenden Bedrohungen und Schwachstellen begegnen			
• Bedrohung: Unbefugter Zugriff	✗	✗	✓
• Schwachstelle: Menschliches Fehlverhalten	✗	✗	✗
Wirtschaftlichkeit und Skalierbarkeit			

Branchenstandard
Bestehende Regulierung im Finanzsektor I/II

Kreditwesengesetz (KWG)

- **Melde-/Anzeige-/Auskunftspflichten** (§ 24, § 44) an Bundesbank und Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)
- **Pflichten zum ordnungsgemäßen Geschäftsbetrieb** (§ 25), daraus folgend MaRisk (Mindestanforderung an das Risikomanagement)
- Anforderungen an die **Jahresabschlussprüfung** (§§ 28-30)
- **Anordnung von Maßnahmen** durch BaFin in besonderen Fällen, z.B. bei Mängeln/Gefahren (§§ 45-48)

Branchenstandard
Bestehende Regulierung im Finanzsektor II/II

Risikoregulierung

- Solvabilitätsverordnung (SolvV)
- Basel II → Capital Requirements Directive (Richtlinie über Eigenkapitalanforderungen), insbes. Richtlinie 2006/48/EG (Bankenrichtlinie)
- Gesetz über den Wertpapierhandel (WpHG)
  + Richtlinie 2004/39/EG (Finanzmarktrichtlinie)
  + Richtlinie 2006/73/EG (Durchführungsrichtlinie zur Finanzmarktrichtlinie)

Internetzahlungen / Onlinebanking

- ECB Recommendations for the Security of Internet Payments (SecuRe Pay) EBA/GL/2014/12
- BaFin Rundschreiben 4/2015: Mindestanf. an die Sicherheit von Internetzahlungen (MaSI)
- BaFin-Schreiben: verpflichtende Zwei-Faktor-Authentifizierung (12/2001)

Aufsicht

- Bundesbank → Chipkarten, electronic cash (POS-Terminals), Clearing-Systeme
- Basler Ausschuss für Bankenaufsicht und Europäische Zentralbank → Großbetrags-Zahlungsverkehr
- Europäische Zentralbank →SEPA-Zahlungsinstrumente Lastschrift und Überweisung

Weitere Gesetze

- BDSG, TMG, GoBD, etc.

Branchenstandard
als Rahmenwerk

- Es gibt bereits viele Regelungen zum Risikomanagement und Einzel-Vorgaben für bestimmte Verfahren, aber keine verpflichtenden übergreifenden IT-Sicherheits-Standards im Finanzsektor
  → Branchenstandard als Rahmenwerk
- Orientierung an Best Practices
  → ISO-Standards

Branchenstandard
Orientierung an ISO-Standards

ISO 2700x: Information technology – Security techniques

- **ISO/IEC 27001:** Information security management systems
  ISO/IEC 27002: Code of practice for inf. security controls
- **ISO/IEC 27005:** Information security risk management
- **ISO/IEC 27015:** ISM guidelines for financial services

ISO/IEC 22301: Societal security – BCM systems

Vorteile:

- **International anerkannt**
- **Freiraum in der Umsetzung**

Branchenstandard
Herausforderungen

- ISO-Standards geben nur den **Rahmen** vor
  – zu entwickeln und ergänzen sind spezifische IT-Sicherheitsmaßnahmen-Vorgaben
- IT-Landschaft, Kritikalität, Unternehmensgrößen etc. sehr **heterogen** – Einigung auf einen für alle angemessenen Umsetzungsgrad des IT-Sicherheitsmanagements schwierig
- Unklarheit, auf welche **Betreiber** die Anforderungen zutreffen werden

Branchenstandard
Aktueller Stand

- Herleitung angemessener Sicherheitsmanagement-Maßnahmen aus ISO-Standards ✓
- Definition eines Meldewegs ✓

Ende 2015

- Ergänzung spezifischer Sicherheitsmaßnahmen ✗
- Beschreibung eines möglichen Prüf-Ablaufs ✗

1. Hj. 2016

Fragen?

Kontakt

SRC
Security Research & Consulting GmbH
Graurheindorfer Str. 149a
53117 Bonn

Tel. **+49-(0)228-2806-170**
Fax: **+49-(0)228-2806-199**
E-Mail: **jana.ehlers@src-gmbh.de**
WWW: **www.src-gmbh.de**