Bundesanstalt für
Finanzdienstleistungsaufsicht

BaFin

Die Umsetzung des IT-Sicherheitsgesetzes durch das BSI-Gesetz – Auswirkungen auf den Bankenbereich

IT-Info - Veranstaltung

16. März 2017

Dr. Jens Gampe

Dr. Sebastian Silberg

Inhaltsübersicht

1. Kontext – Kritische Infrastrukturen
2. Rechtliche Einordnung
3. Aufsichtliche Umsetzung durch Kritis-VO
4. Implikationen für die Kreditwirtschaft

IT-Sicherheit in Europa, Deutschland und im Finanzsektor

1. Kontext – Kritische Infrastrukturen

Kontext → Pressemeldungen

BaFin

Cyber-Angriff auf Bitcoin-Bank Inputs.io: Kunden verlieren ihr Geld (2013, Deutsche Wirtschafts Nachrichten)

Trojaner-Angriff auf den Bundestag: Cyper-Spione kaperten offenbar wichtige Computer der Regierung (2015, Focus)

Datenklau bei Großbank JP Morgan (2014, n-tv)

Cyber-Kriminalität – sorglose Mitarbeiter sind das Kernproblem (2016, IT Finanzmagazin)

Cyber-Kriminalität Hacker plündern 20.000 Girokonten in Großbritannien (2016, FAZ)

Milliardenschäden durch Cyber-Angriffe auf deutsche Wirtschaft (2012, FAZ)

Zahlungssystem Swift meldet erneut Angriff auf eine Bank (2016, Zeit)

UP KRITIS – Public Private Partnership

BaFin

Sicherstellung der Grund-versorgung der Bevölkerung

Gemeinsame Verantwortung von Staat und Wirtschaft

UP KRITIS

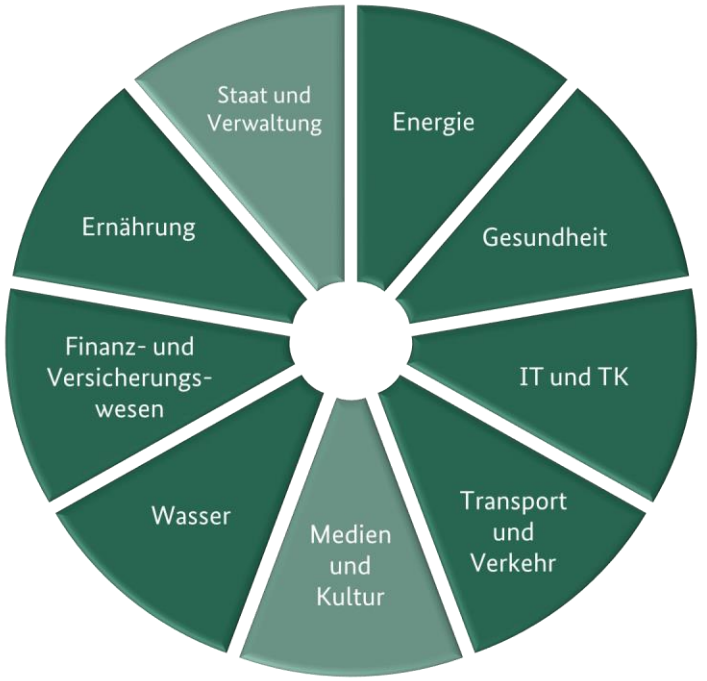
seit 2004

Informationstechnologie ist Schwerpunkt

Essentieller Beitrag zum Schutz der Kritischen Infrastrukturen

Kontext → KRITIS - Sektoren

- spezieller Fokus auf Versorgungssicherheit, insb. der Bevölkerung



- Finanzsektor einer von 8 kritischen Sektoren, hier Fokus insb. auf die Verfügbarkeit der Zahlungssysteme

Teilnehmer UP KRITIS (Auswahl)

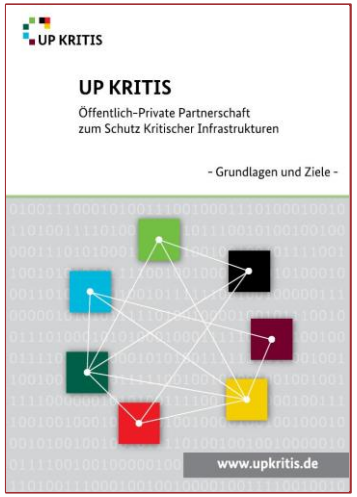
Quelle der Grafik: BSI

Quelle: BSI

Kontext → Zeitschiene

BaFin

UP KRITIS

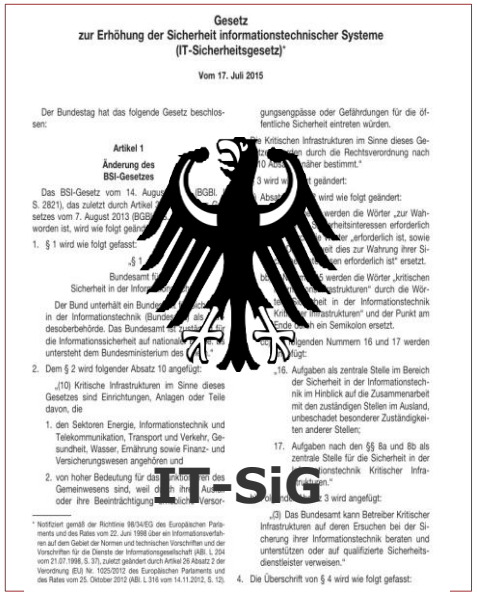


2014

2013

2011

2005



2015

2013

Kontext → NIS-Richtlinie

Netz- und Informationssysteme müssen verlässlich und sicher sein:

- sie haben eine zentrale Rolle in der Gesellschaft,
- sie sind unerlässlich für das reibungslose Funktionieren des Binnenmarkts,
- insbes. das Internet spielt eine tragende Rolle bei der Erleichterung des grenzüberschreitenden Waren-, Dienstleistungs- und Personenverkehrs,
- schwere Störungen solcher Systeme — unabhängig davon, ob sie beabsichtigt oder unbeabsichtigt sind und wo sie auftreten — können einzelne Mitgliedstaaten und die Union insgesamt in Mitleidenschaft ziehen.

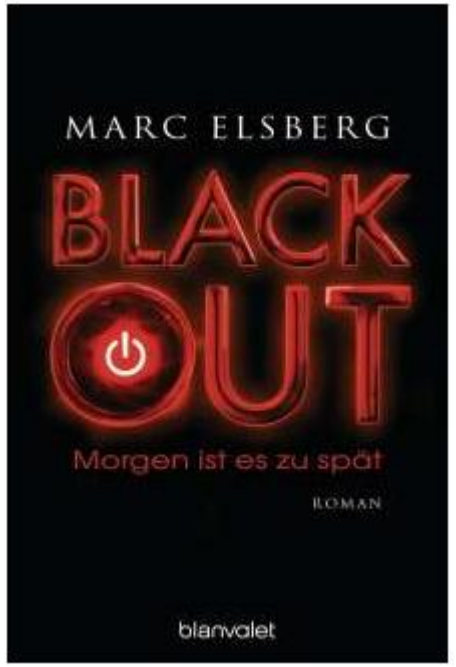
Kontext → IT-Sicherheitsgesetz

Kritische Infrastrukturen (KRITIS)
sind Organisationen/Einrichtungen

- mit **wichtiger Bedeutung für das Gemeinwesen**,
- deren Ausfall oder Beeinträchtigung
- nachhaltig wirkende Versorgungsengpässe,

erhebliche Störungen der öffentlichen Sicherheit oder

andere dramatische Folgen nach sich ziehen würde.



„Blackout" (Cover, 2012)
gem. CC BY-SA 3.0 de

IT-SiG wird durch Novellierung des BSI-Gesetzes umgesetzt

2. Rechtliche Einordnung

BSIG – maßgebliche Paragraphen

IT-SiG als Artikelgesetz konzipiert, u.a. BSIG betroffen:

- § 2 - Begriffsbestimmungen, u.a. KRITIS
- § 3 - Aufgaben des Bundesamtes
- § 8a - Sicherheit in der Informationstechnik Kritischer Infrastrukturen
- § 8b - Zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen
- § 10 - Ermächtigung zum Erlass von Rechtsverordnungen
- § 14 - Bußgeldvorschriften

BSIG – maßgebliche Paragraphen
§ 8a

BaFin

- Verpflichtung der Betreiber Kritischer Infrastrukturen gemäß Absatz 1, angemessene Vorkehrungen zur Sicherstellung der *Verfügbarkeit*, *Integrität, Authentizität und Vertraulichkeit* ihrer informationstechnischen Systeme zu treffen
- Frist: Erstmals innerhalb von zwei Jahren nach Inkrafttreten der Verordnung, hernach mindestens alle zwei Jahre entsprechender Nachweis
- Nachweis insbesondere durch Sicherheitsaudits, Prüfungen oder Zertifizierungen
- Einhaltung des Stands der Technik (Soll-Bestimmung)

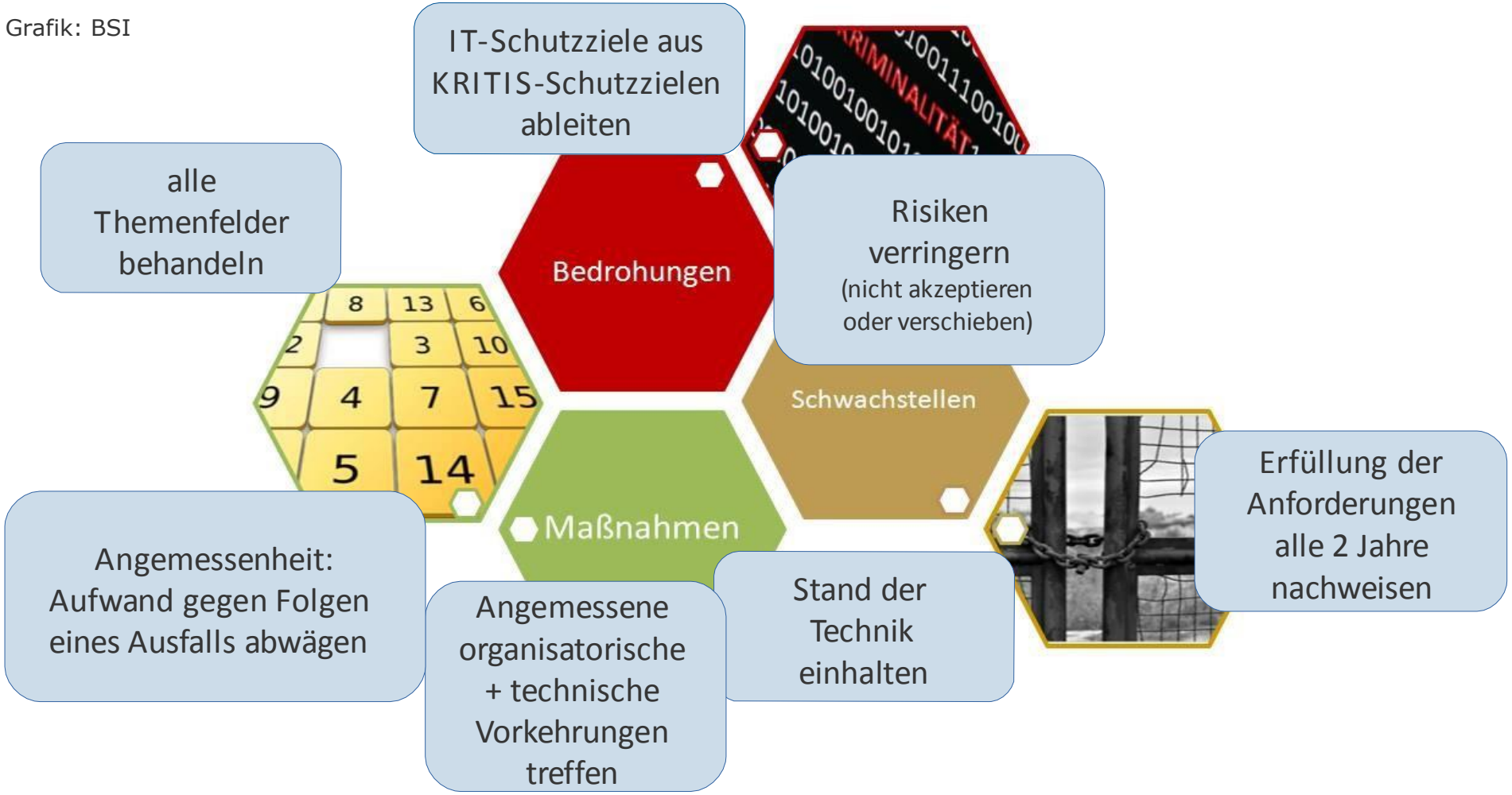
BSIG – maßgebliche Paragraphen
§ 8a

BaFin

- Erarbeitung und Einreichung eines branchenspezifischen Sicherheits-Standards (B3S) möglich
- Feststellung der Eignung von durch Betreiber Kritischer Infrastrukturen oder ihre Verbände vorgeschlagenen branchenspezifischen Sicherheits-Standards (B3S) zur Erfüllung der Anforderungen gemäß § 8a Abs. 1 BSIG durch das BSI im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes
- Im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes ggf. Beseitigungsverlangen des BSI im Fall von festgestellten Sicherheitsmängeln

Anforderungen gemäß § 8a BSIG → es geht um KRITIS!

Quelle der Grafik: BSI



Themenfelder

Quelle der Grafik: BSI (rote Hervorhebungen durch BaFin)

BSIG – maßgebliche Paragraphen
§ 8b

Anforderungen an Betreiber Kritischer Infrastrukturen:

- Verpflichtung zur Einrichtung einer Kontaktstelle
- Sicherstellung der jederzeitigen Erreichbarkeit
- Verpflichtung zur unverzüglichen Meldung erheblicher Störungen

BSIG – maßgebliche Paragraphen
§ 8b

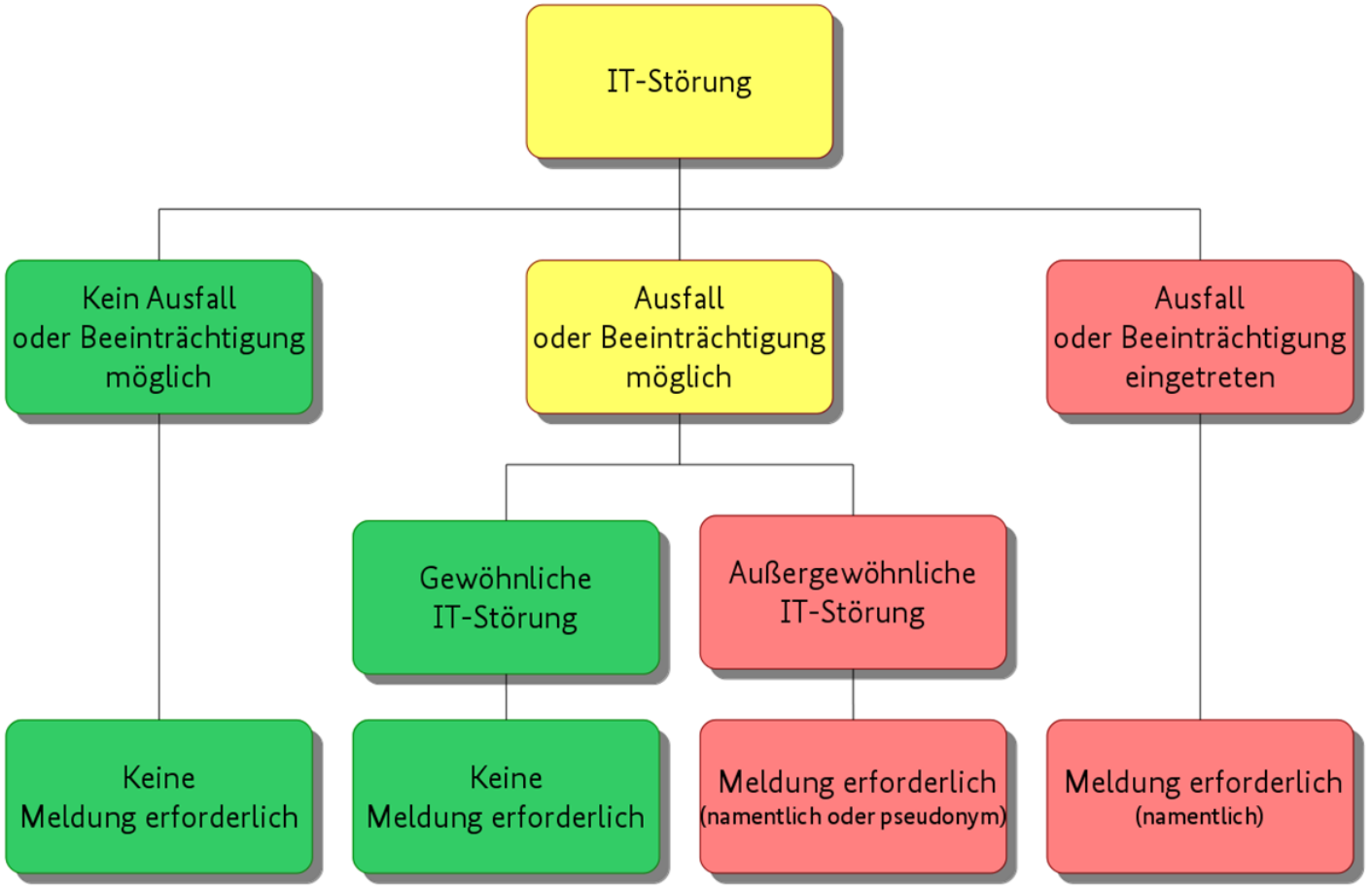
BaFin

Aufgaben des BSI:

- Sammlung wesentlicher Informationen, Auswirkungsanalyse in Zusammenarbeit mit zuständiger Aufsichtsbehörde und Erstellung eines Lagebildes
- Unverzügliche Unterrichtung der Betreiber Kritischer Infrastrukturen über sie betreffende Informationen sowie der zuständigen Aufsichtsbehörden des Bundes über die zur Erfüllung ihrer Aufgaben erforderlichen Informationen

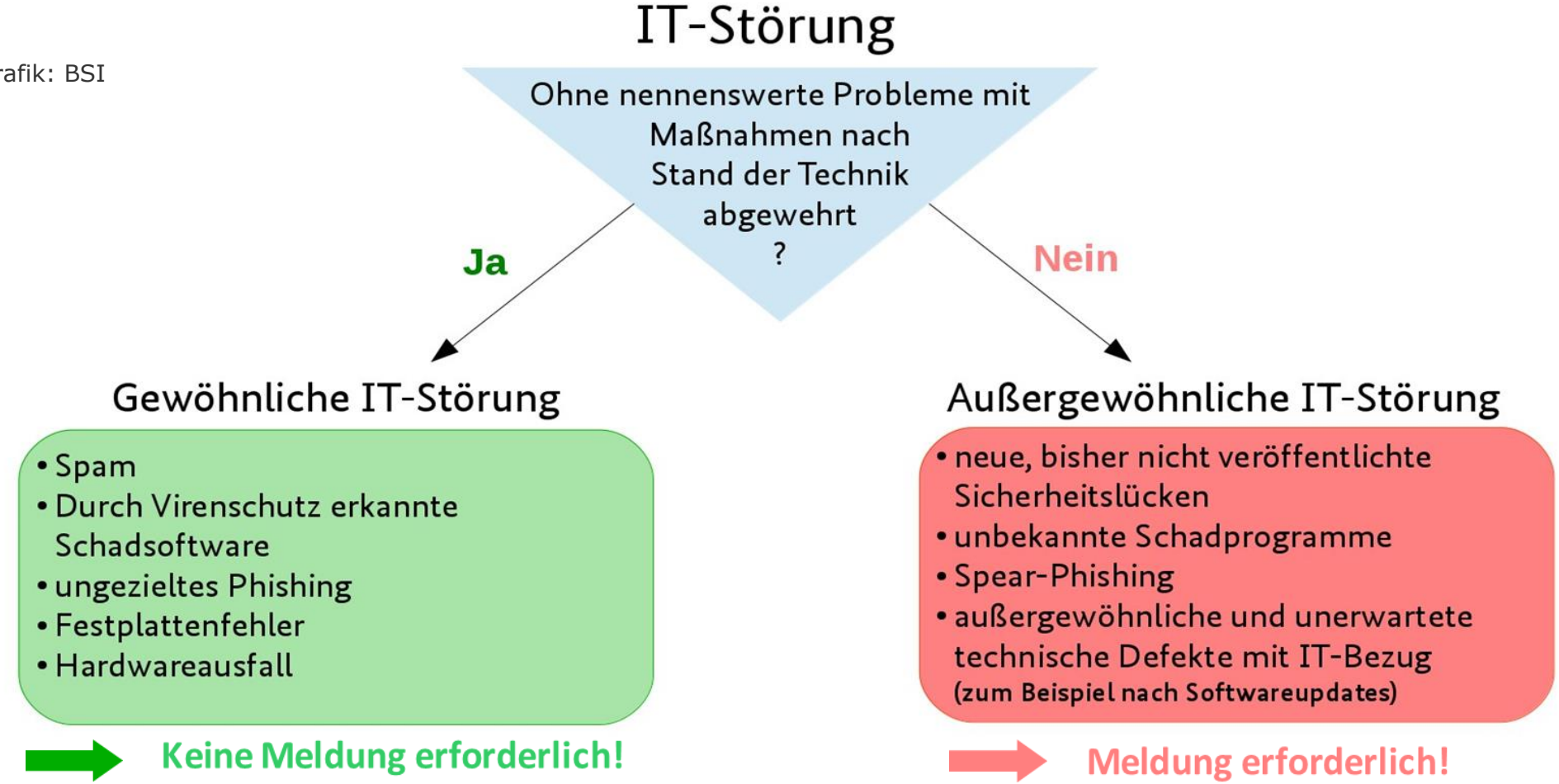
BSIG – maßgebliche Paragraphen
§ 8b

Quelle der Grafik: BSI



BSIG – maßgebliche Paragraphen
§ 8b

Quelle der Grafik: BSI



BSIG – maßgebliche Paragraphen §§ 10, 14

BaFin

- § 10: Verordnungsermächtigung (Identifizierung der Betreiber Kritischer Infrastrukturen): Festlegung von kritischen Dienstleistungen im Sektor, Anlagen sowie Schwellenwerten
- § 14: Bußgeldvorschrift (Geldbuße bis zu 100.000 € im Falle von Verstößen gegen bestimmte Anforderungen der §§ 8a, 8b BSIG möglich)

BSIG wird durch Kritis-Verordnung konkretisiert

3. Aufsichtliche Umsetzung

BSIG-Umsetzung durch die Kritis-VO

- In 2016/2017 Erarbeitung der Rechtsverordnung zur Identifizierung der Betreiber Kritischer Infrastrukturen, u.a. im Finanzsektor, unter Vorsitz des BMI.
- Mitwirkung erfolgte seitens BMF, BaFin, BSI sowie Vertretern der Kreditwirtschaft (Kernteam).
- Inkrafttreten der Änderungs-VO für 2. Quartal 2017 geplant.

BSIG-Umsetzung durch die Kritis-VO
Betreiberbegriff:

- Betreiber ist eine natürliche oder juristische Person, die unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände bestimmenden Einfluss auf die Beschaffenheit und den Betrieb einer Anlage oder Teilen davon ausübt.
- Abweichend von § 1 Nr. 2 Kritis-VO hat gemäß Änderungs-VO-Entwurf im Sektor Finanz- und Versicherungswesen bestimmenden Einfluss auf eine Kritische Infrastruktur, wer die **tatsächliche Sachherrschaft ausübt**.
  Die rechtlichen und wirtschaftlichen Umstände bleiben insoweit unberücksichtigt.

BSIG-Umsetzung durch Kritis-VO

Unternehmen müssen sich **selbst identifizieren** und anschließend beim BSI melden!

Identifizierungsprozess:

1. Kritische Dienstleistungsbereiche,
2. Anlagekategorien,
3. Schwellenwerte auf Basis der Bemessungskriterien.

BSIG-Umsetzung durch Kritis-VO
Kritische Dienstleistung: Zahlungsverkehr

BaFin

Als kritisch für den Bankenbereich wurden folgende drei Dienstleistungsbereiche identifiziert:

1. Bargeldversorgung,
2. Bargeldloser Zahlungsverkehr (Karten),
3. konventioneller Zahlungsverkehr (Überweisung/Lastschrift),
4. *Verrechnung und Abwicklung von Wertpapier- und Derivatgeschäften,*
5. *Versicherungsdienstleistungen*.

BSIG-Umsetzung durch Kritis-VO
Beispiel

BaFin

Der für die Anlagenkategorien des Teils 3 Nummer 2.1.1 bis 2.2.2 und 2.3.1 genannte Schwellenwert ist unter Annahme von 42 Transaktionen mit im Inland ausgegebenen Karten an Terminals (POS) in- und ausländischer Zahlungsdienstleister und eines Regelschwellenwertes von 500 000 versorgten Personen wie folgt berechnet:

42 Transaktionen/Jahr x 500 000 = 21 Millionen Transaktionen/Jahr

Zusammenarbeit
BSI - BaFin

4. Implikationen für die Kreditwirtschaft

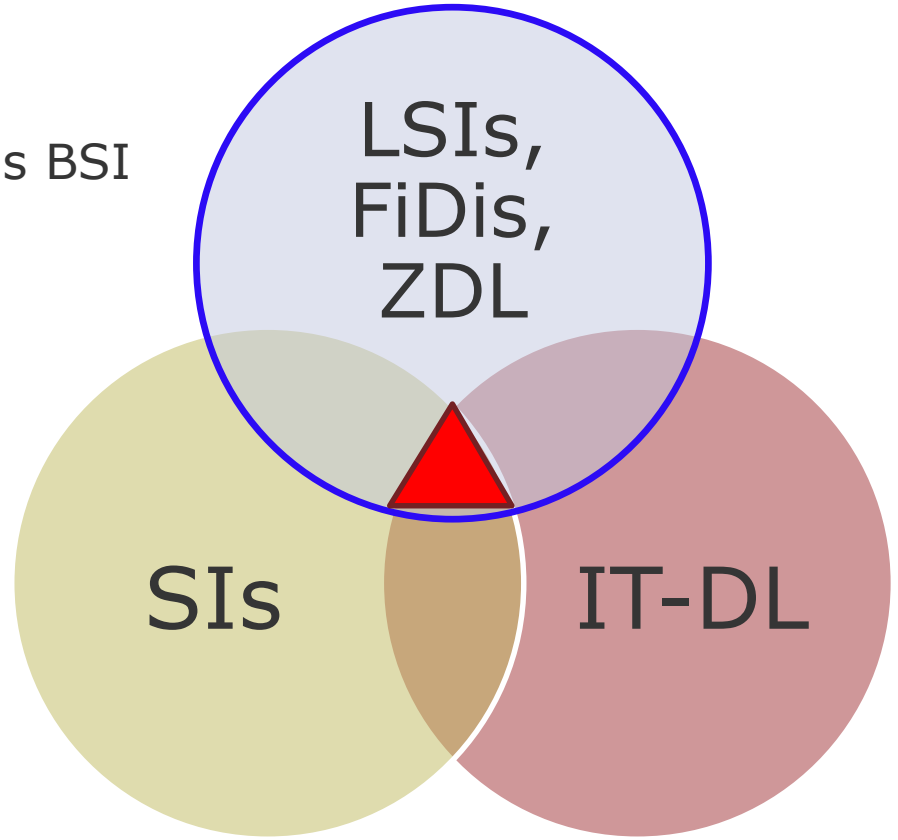
BSIG-Umsetzung durch Kritis-VO
Zusammenarbeit BSI - BaFin

BaFin

Duale Aufsicht:

- verknüpft
  - das technische Spezialwissen des BSI
- mit dem
  - branchenspezifischen Fachaufsichtswissen der BaFin

in Deutschland



BSIG-Umsetzung durch Kritis-VO
BAIT vs. B3S

BaFin

- BAIT werden für alle KWG-Aufsichtsobjekte unmittelbar gelten sowie für IT-DL als Auslagerungsunternehmen mittelbar
- freiwillig kann sich jeder Kritis-Betreiber (Zahlungsverkehr) gegen den B3S mappen und ihn auch beim BSI einreichen (wer einreicht, bindet sich grundsätzlich selbst)
  - Hieran knüpft ggf. der Nachweis der angemessenen org. Vorkehrungen zur Vermeidung von VIVA-Störungen (Audits/Prüfungen/Zertifikate vs. JAPB, § 13 PrüfBV)

BSIG-Umsetzung durch Kritis-VO Meldepflichten

- Gemäß PSD2-Umsetzungsgesetz Meldepflicht für alle ZDL

- Gemäß BSIG Meldepflicht nur für Kritis-Betreiber (tatsächliche Sachherrschaft über entsprechende Anlage)

  - Unterschiedliche gesetzliche Adressaten (ZAG [neu] vs. BSIG)
  - Unterschiedliche Meldeformulare (EBA vs. BSI)
  - Unterschiedliche Meldeinhalte wg. unterschiedlicher Ziele (Verfügbarkeit der ZV-Systeme vs. Kritis-Lagebild)

BSIG-Umsetzung durch Kritis-VO Zusammenfassung

BaFin

Kritisches Institut im Sinne der Kritis-VO ist im Bankensektor (Zahlungsverkehr):

- Betreiber einer Anlage /Teil einer Anlage, die einer Anlagen-kategorie (gem. Anhang 6/Teil 3 Spalte B) zuzuordnen ist

und

- Erreichen oder Überschreiten des Schwellenwertes (gem. Teil 3 Spalte D)

Nur für diese gelten neben den KWG-Anforderungen der BaFin auch die Normen des BSIG

Vielen Dank!

BaFin

Ihre Ansprechpartner:

Dr. Jens Gampe

Tel. +49 (0)228 / 4108-2332

jens.gampe@bafin.de

Dr. Sebastian Silberg

Tel. +49 (0)228 / 4108-1622

sebastian.silberg@bafin.de

Referat BA 51 - Kompetenz IT-Sicherheit