BaFin

Bundesanstalt für
Finanzdienstleistungsaufsicht

Arbeitsschwerpunkte 2018 der Gruppe IT-Aufsicht

IT-Aufsicht bei Banken 27.09.2018

Gruppe IT-Aufsicht/ Zahlungsverkehr/ Cybersicherheit

Gruppe IT- Aufsicht / Zahlungs-verkehr/Cybersicherheit
GL: N.N.
i.V. Jens Obermöller

GIT 1

Grundsatz Cybersicherheit in der Digitalisierung und Regulierung Zahlungsverkehr

RL: Jens Obermöller

GIT 2

Operative Aufsicht über Zahlungsinstitute und E-Geld-Institute

RL´in: Monika Herpers

GIT 3

Grundsatz IT-Aufsicht und Prüfungswesen

RL´in: Ira Steinbrecher

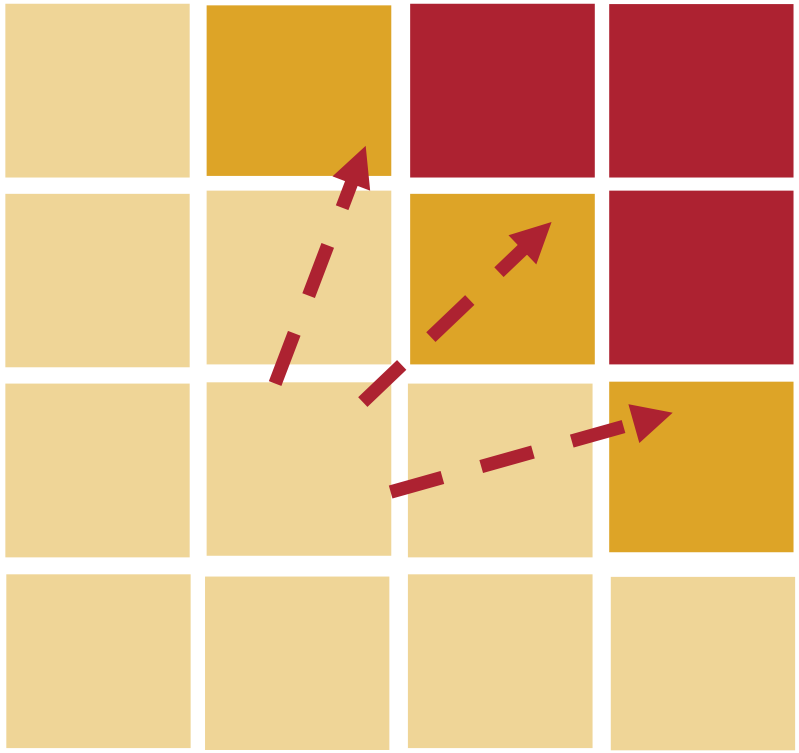
GIT 4

IT-Prüfungen und Prüfungs-/ Aufsichtsunterstützung

RL: N.N.
i.V. Renate Essler

Einschätzung der Bedeutung von IT-/Cyberrisiken-auf Einzelinstitutsebene

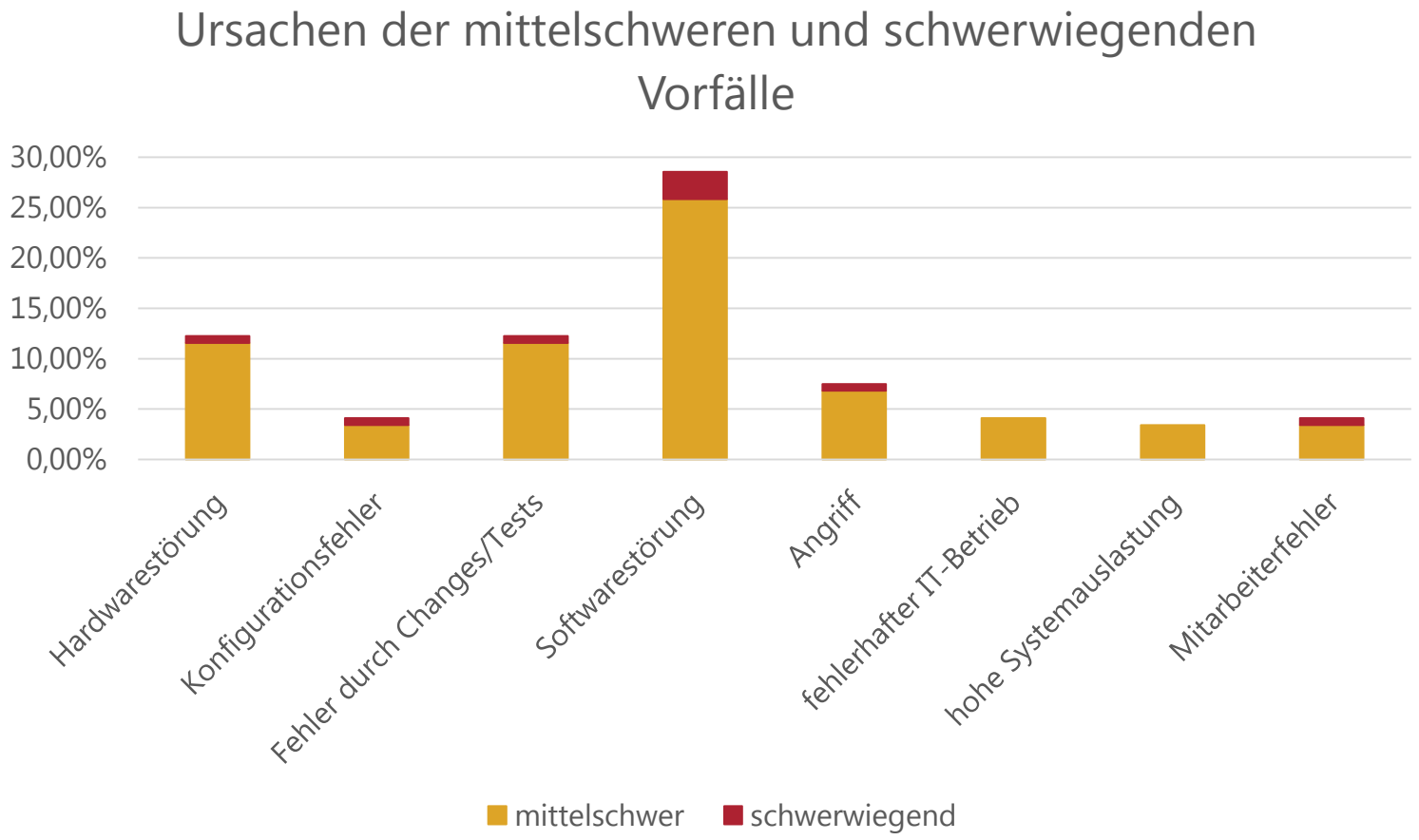
Auswirkung auf Einzelinstitut hoch



Untermauert durch die deutsch-französischen IT-Sicherheitslagebilder von BSI und ANNSI sowie verfügbare Sicherheitsstudien. Grundsätzlich wird von weiter zunehmenden Bedrohungslage insbesondere durch destruktiver Angriffe ausgegangen (bspw. durch Ransomware).

Häufigkeit bei Einzelinstituten hoch

Ursachen für Sicherheitsvorfälle - Erkenntnisse aus dem Meldewesen



- seit 2017 rund 420 Sicherheitsvorfallsmeldungen (MaSi bzw. PSD 2), davon rund ein Drittel mittelschwere und schwere Vorfälle
- Mängel im Bereich der „Cyberhygiene“ als eine wesentliche Ursache
- nur wenige Vorfälle durch Cyberangriffe verursacht

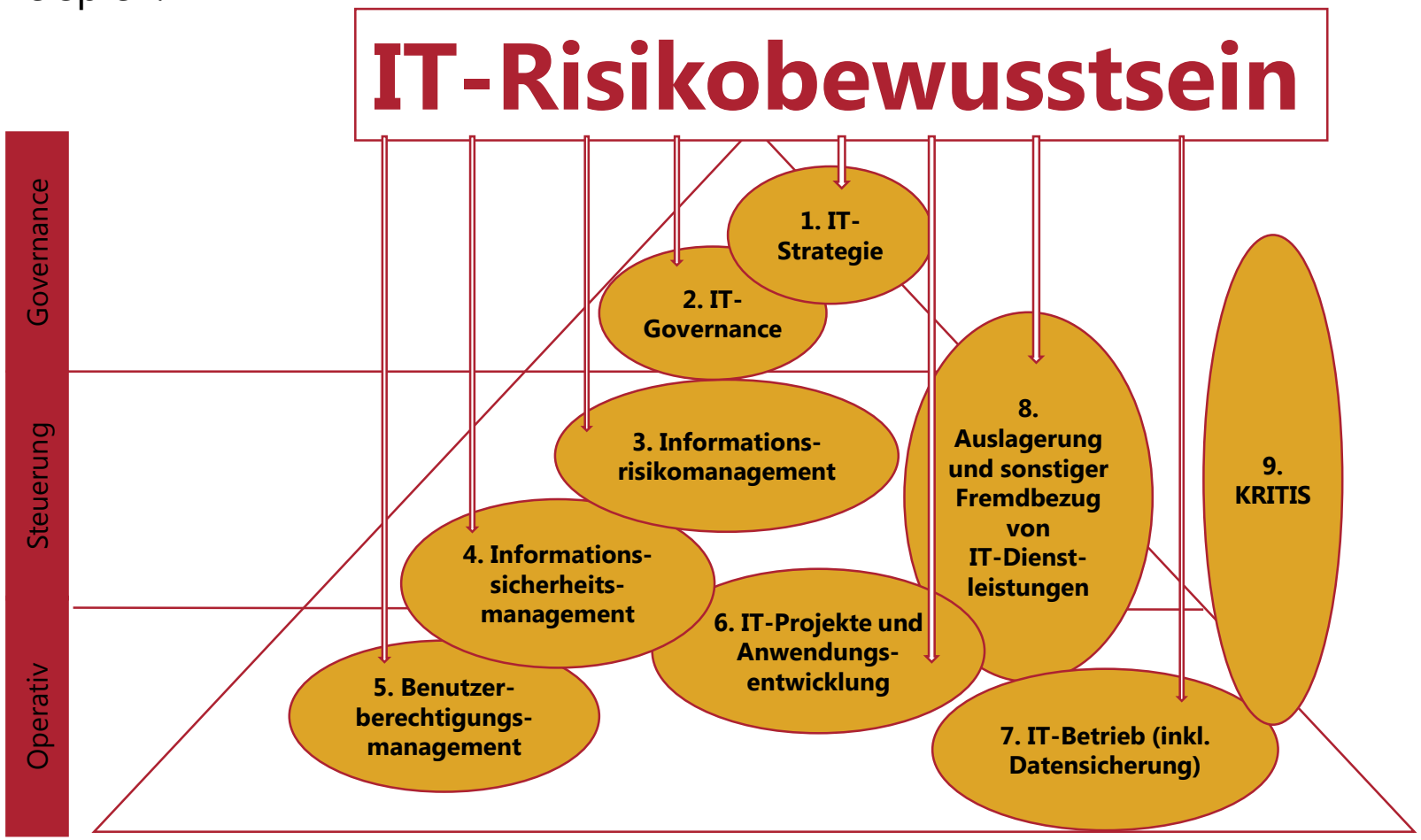
Informations-/Cybersicherheit – sektorweite Schwachstellen

Häufig beobachtbare Schwachstellen – eine europäische Sicht:

- unzureichende „Cyber-Hygiene“
- unzureichende Überwachung von dritten Dienstleistern bzw. der Lieferkette
- unzureichendes Testen von Prozessen, Technologien, aber auch Personen
- unzureichende Investitionen in die Fähigkeiten, Cyber-Angriffe zu entdecken und Bedrohungen zu identifizieren
- unzureichende strategische Planung und strategische Steuerung im Bereich Cyber
- Gegenwart von „End-of-Life“ – Systemen
- technikzentrierter Fokus, Faktor Mensch wird vernachlässigt

Aufsichtliche Anforderungen als eine Antwort

Beispiel : BAIT



Aufsichtliche Anforderungen wie die BAIT adressieren wesentliche Problembereiche bereits heute.

Vor dem Hintergrund der Risikolage und der stabilen Befunde im Bereich der beobachteten Schwachstellen rücken aber Fragen der **Kontinuität und Resilienz der IT** weiter in den Vordergrund.

Überblick EBA – Arbeiten mit IT - Bezug

Guidelines on ICT Assessment under the Supervisory Review and Evaluation process (SREP)

(Status: Veröffentlicht; Integration in die Verwaltungspraxis zur Erstellung von Risikoprofilen)

Die Leitlinien ergänzen die bestehenden SREP-Leitlinien um ein Vorgehensmodell mit expliziten Basisanforderungen zur Analyse und Bewertung von IT-Risiken.

Recommendations on outsourcing to Cloud Service Providers

(Status: Veröffentlicht; Integration in die Überarbeitung der EBA GL on Outsourcing)

Themenbereiche der seit Juni 2018 geltenden Recommendations sind u.a. Beurteilung der Wesentlichkeit, Informationspflichten gegenüber der Aufsicht und Prüfungsrechte für Banken und die Aufsicht, Geographische Lage der Daten/ -verarbeitung, Weiterverlagerungen sowie Ausstiegsklauseln

Überblick EBA – Arbeiten mit IT - Bezug

Überarbeitung CEBS - Guidelines on Outsourcing

(Status: Entwurf der Leitlinien konsultiert – Konsultationsfrist endete am 24.09.2018)

- Fortschritt in der Informationstechnologie und europarechtlichen Vorgaben aus CRD IV, MiFiD, AMLD und PSD 2 machen eine Aktualisierung notwendig.
- Der Entwurf sieht vor, dass Institute ein Auslagerungsregister über „wesentliche“ und „unwesentliche“ Auslagerungen führen. Diese sollen der Aufsicht auf Anfrage zur Verfügung gestellt (bspw. zur Identifikation von Konzentrationsrisiken) bzw. in den SREP-Prozess implementiert werden.
- Eine solche Übersicht ist in der Praxis nicht neu (auch die PrüfbV enthält hierzu eine Erfordernis). Allerdings variiert die Qualität und Format solcher Repositorien in der Praxis signifikant.
- Die bereits letztes Jahr verabschiedeten **„EBA Recommendations on outsourcing to cloud service providers“** wurden in die neuen Leitlinien integriert.

Überblick EBA – Arbeiten mit IT - Bezug

Guidelines on ICT Risk Management

(Status: in Bearbeitung)

Die Leitlinien sollen die Erwartungshaltung an das Management der IT-Risiken in den Instituten wiedergeben.

Die Einbeziehung der EBA **„Leitlinien zu Sicherheitsmaßnahmen bezüglich der operationellen und sicherheitsrelevanten Risiken von Zahlungsdiensten gemäß der Richtlinie (EU) 2015/2366 (PSD2)“** wird geprüft.

Veröffentlichung eines Konsultationsentwurfs ist für Ende 2018 vorgesehen

Überblick EBA – Arbeiten mit IT - Bezug

PSD 2-Maßnahmen mit Bezug zur Informationssicherheit

(soweit noch nicht behandelt)

Leitlinien für die Meldung schwerwiegender Vorfälle

- in Deutschland durch BaFin Rundschreiben 08/2018 (BA) zur Meldung schwerwiegender Zahlungs-sicherheitsvorfälle vom 07.06.2018 umgesetzt
- hat die Meldungen nach MaSI ersetzt; bitte **nicht** mehr das MaSI-Formular benutzen

RTS on Strong Customer Authentication and common and secure communication

- als Delegierte Verordnung (EU) 2018/389 unmittelbar anwendbares Recht ab dem **14.09.2019**

Guidelines on Fraud Reporting

- englische Fassung am 18.07.2018 veröffentlicht
- Übernahme in Deutschland wird geprüft

Cybersicherheit – ausgewählte internationale Initiativen

G7 Cyber Expert Group

In 2015 gegründet mit dem Ziel, Kooperation & Austausch zwischen den Mitgliedstaaten zu verstärken und die Cybersicherheit im Finanzsektor zu erhöhen.

- **Fundamental Elements of Cybersecurity (FEC):** ein generisches Rahmenwerk acht grundlegender Elemente für die Erhöhung der Cybersicherheit im gesamten Finanzsektor, Ende 2016 veröffentlicht.

- **Fundamental Elements for Effective Assessment**: ergänzen die FEC um grundlegende Elemente und eine Methodologie zur Abschätzung der Effektivität von Cybersicherheitsmaßnahmen, Ende 2017 veröffentlicht.

Laufende Arbeiten der G7-Expertengruppe: Risiken durch Drittparteien; Threat Led Penetration Testing (Red Teaming) ; Cross Border Exercising sowie Koordination mit anderen Sektoren

Cybersicherheit – ausgewählte internationale Initiativen

Financial Stability Board – Cyber Lexicon Working Group (CLWG)

Die CLWG wurde auf Initiative der G20 Finanzminister 2017 gegründet.
Ziel ist, im Rahmen eines Lexikonprojektes ein gemeinsames Verständnis und eine gemeinsame Terminologie für relevante Begriffe aus den Themenbereichen Cyber-Sicherheit und Cyber-Resilienz zu erarbeiten.

Das Cyber-Lexikon soll die Arbeiten und den Informationsaustausch im Bereich Cybersicherheit unterstützen. Es richtet sich an alle Akteure im Finanzsektor aber auch internationale Standardsetzer

Ein Entwurf, bestehend aus 50 Kernbegriffen, wurde bis August 2018 öffentlich konsultiert. Eine Veröffentlichung des FSB Cyber-Lexikons ist für Ende 2018 geplant.