T.I.S.P.
TeleTrusT Information Security Professional

TeleTrusT
Pioneers in IT security.

T.I.S.P. Community Meeting

Berlin, 06. - 07.11.2018

IT-Sicherheitsgesetz, PSD II & Co.: Regulatorische Anforderungen und Auswirkungen auf das 'Daily Business'

Ernst-Heinrich Paap (IT-Sicherheitsmanager),
Hamburger Sparkasse

Inhalt

1. Kurze Vorstellung der Haspa
2. IT-Compliance für Banken und Sparkassen (Überblick)
3. Wer reguliert die Banken und Sparkassen ?
4. Regulatorische Anforderungen aus …
   a. MaRisk und BAIT
   b. PSD 2
   c. IT-Sicherheitsgesetz (KRITIS)
5. Schlusswort und Fazit

Die Haspa auf einen Blick.

- 1827 gegründet
- Über 40 Mrd. Euro Bilanzsumme
- Rund 5.000 Mitarbeiter und 350 Ausbildungsplätze
- 1,5 Millionen Kunden
- Breit gefächertes Angebot von Finanzdienst-leistungen für alle Kundengruppen in 28 Regionen
- Flächendeckendes Standortnetz
  - Rund 150 Filialen
  - Rund 50 SB-Standorte
  - Rund 40 Firmenkunden-Standorte
  - 2 Private-Banking-Standorte
- Vielfältiges gesellschaftliches Engagement: Rund 5 Mio. Euro jährlich für Bildung, Soziales, Kunst, Musik und Sport

Haspa Zentrale am Adolphsplatz

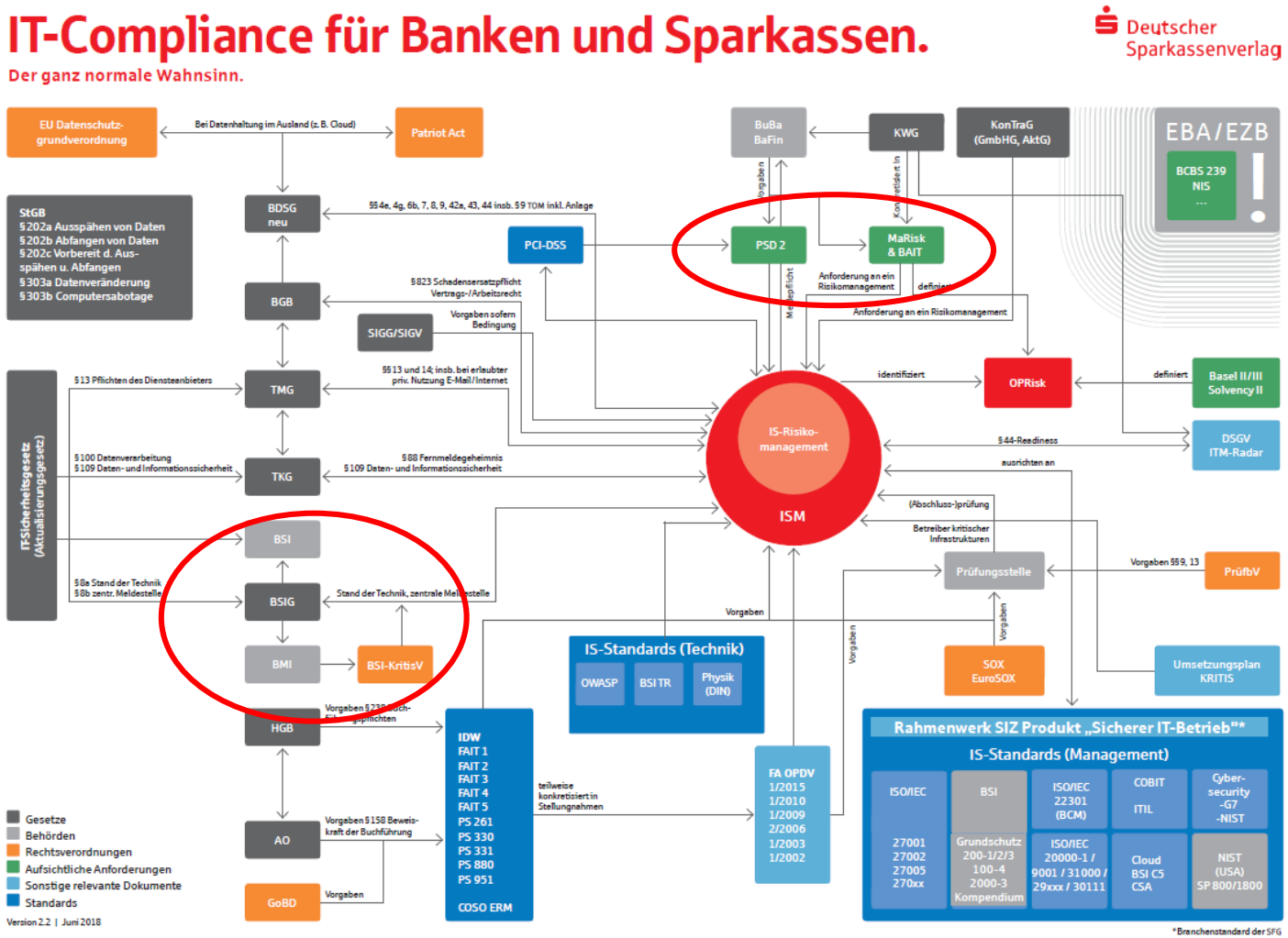
Haspa Filiale

Haspa
Hamburger Sparkasse

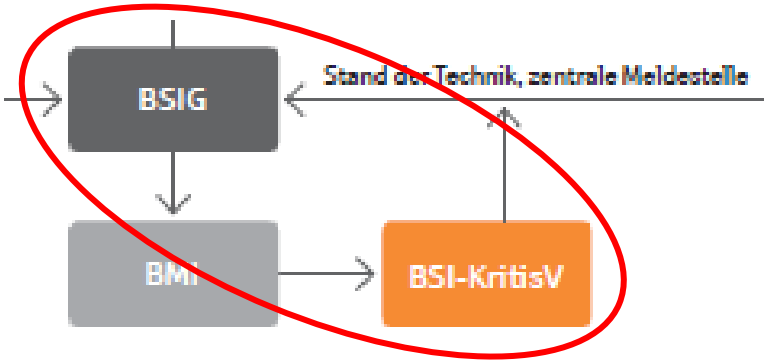
Zu meiner Person

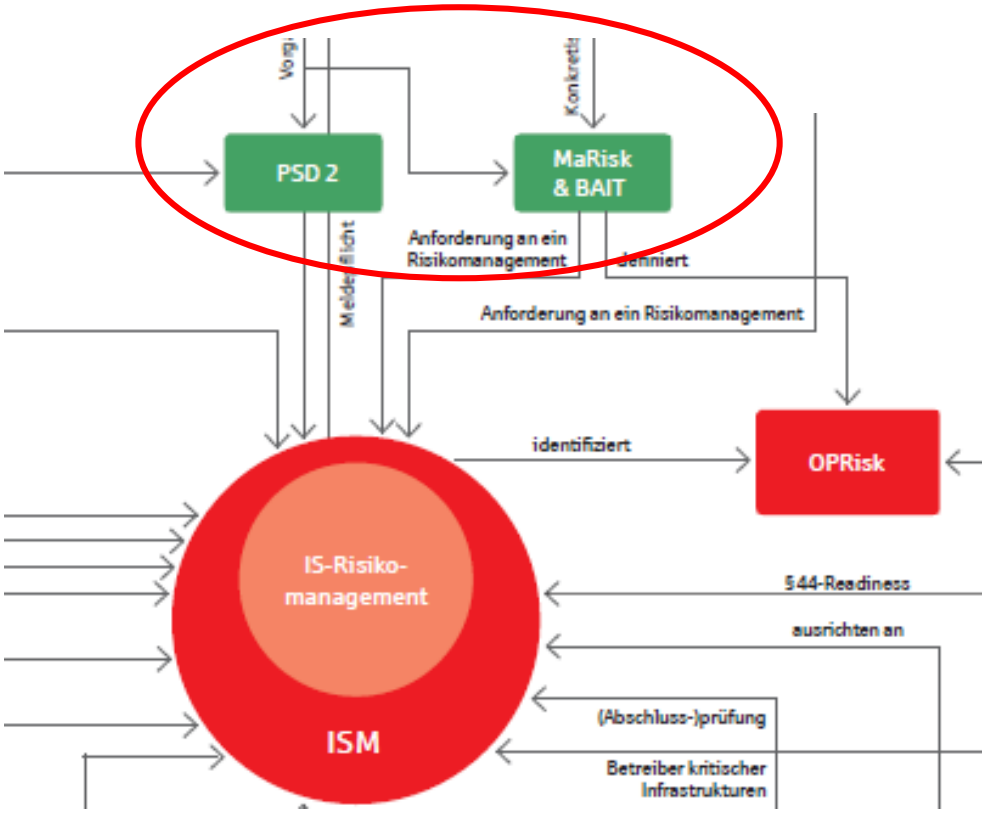
- Studium der Physik an der Universität Hamburg mit Abschluss Diplom-Physiker
- 18 Jahre Tätigkeiten in Unternehmen des Rüstungsbereiches (Marineprojekte)
- Seit Mai 1999 als IT-Sicherheitsmanager in der Haspa tätig
- Tätigkeitsschwerpunkte:
  - Notfall- und Wiederanlaufplanung
  - Erarbeitung von Konzepten und Risikoanalysen zu diversen Themen und Projekten
  - Begleitung und Steuerung von Audits zu technischen Fragestellungen
  - Steuerung von IT-Dienstleistern
  - Cyber-Kriminalität (Online-Betrug / Phishing) und Cyber-Angriffe

Gesetzliche und aufsichtsrechtliche Anforderungen



Gesetzliche u. aufsichtsrechtliche Anforderungen (Auszug)





ISM = Informationssicherheitsmanagement

Wer reguliert die Banken in Deutschland?

Auf nationaler Ebene

- Bundesbank
- Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)

Auf europäischer Ebene in Abstimmung mit den nationalen Behörden

- Europäische Zentralbank (EZB)
- European Banking Authority (EBA)

Regelungen für Kritische Infrastrukturen durch das IT-Sicherheitsgesetz

- Bundesamt für Sicherheit in der Informationstechnik (BSI)

Regulatorik durch die BaFin: MaRisk

Mindestanforderungen an das Risikomanagement

- Rundschreiben der BaFin mit Pflicht zur Einhaltung
- Regelt u.a. die Anforderungen an das Risikomanagement
- Anforderungen an die technisch-organisatorische Ausstattung
  - Berechtigungsmanagement
  - Trennung von Test und Produktion
  - Angemessene Überwachungs- und Steuerungsprozesse für IT-Risiken
- Notfallkonzept
  - Vorsorge für Notfälle zeitkritischer Aktivitäten und Prozesse
  - Im Falle von Auslagerungen müssen die Notfallpläne des auslagernden Instituts und des Auslagerungsunternehmens aufeinander abgestimmt sein
- Auslagerung von Dienstleistungen: umfassendes Kapitel mit Anforderungen

Regulatorik durch die BaFin: BAIT

Bankaufsichtliche Anforderungen an die IT

- Rundschreiben der BaFin mit Pflicht zur Einhaltung
- Konkretisierung der Anforderungen aus der MaRisk
- Formulierung von Anforderungen in 9 Abschnitten zu
  - IT-Strategie
  - IT-Governance
  - Informationsrisikomanagement
  - Informationssicherheitsmanagement
  - Benutzerberechtigungsmanagement
  - IT-Projekte, Anwendungsentwicklung
  - IT-Betrieb (inkl. Datensicherung)
  - Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen
  - Kritische Infrastrukturen

Inhalte der BAIT (auszugsweise)

Die Anforderungen haben regelmäßige Umsetzungsaufwände zur Folge (Prozessgedanke, PDCA-Zyklus)

- IT-Strategie → Vorgabe von Mindestinhalten
- IT-Governance → Forderung nach angemessener Personalausstattung von IT-Risiko- und IT-Sicherheitsmanagement
- Informationsrisikomanagement
  - → Überblick über Bestandteile des Informationsverbundes
  - → Forderung eines Sollmaßnahmenkatalogs zur Umsetzung der Schutzziele
  - → Regelmäßige Berichterstattung an die Geschäftsleitung (mindestens vierteljährlich)
- Informationssicherheitsmanagement
  - → Informationssicherheitsbeauftragter

Inhalte der BAIT (auszugsweise)

- Benutzerberechtigungsmanagement
  → Vorgaben zu nicht personalisierten Berechtigungen
  → Vorgaben zu Berechtigungsprozessen

- IT-Projekte, Anwendungsentwicklung
  → Berücksichtigung von Projektrisiken im Risikomanagement
  → Vorgaben zur Anwendungsentwicklung (prozessural)

- …

- Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen
  → Risikobewertungen und Vertragsgestaltung

- Kritische Infrastrukturen
  → Nachweiserbringung gem. § 8a, Abs. 3, BSIG

PSD 2 (EZB / EBA)

Payment Service Directive 2 (2. Zahlungsdiensterichtlinie)

- Regulierung neuer Zahlungsdienste
  (Zugriff autorisierter Drittdienstleister auf online geführte Zahlungskonten)

- Meldepflichten der Kreditinstitute über Zahlungsverkehrsausfälle

- Meldeportal der BaFin
  - Schaffung neuer Prozesse innerhalb der Institute
    (wer ist fachlich verantwortlich, wer bewertet, wer meldet? …)
  - Durchführung von Meldungen
  - Dokumentation der gemeldeten Ausfälle

Meldekriterien für PSD 2: Ausfall Zahlungsverkehr

Mind. einmal hohe Schwelle oder mind. dreimal niedrige Schwelle gerissen bedeutet Melden

SIZ

Kriterium	Niedrige Schwelle	Hohe Schwelle
Betroffene Transaktionen	> 10 % der üblichen Transaktionen **und** > 100.000 €	> 25 % der üblichen Transaktionen **oder** > 5.000.000 €
Betroffene Kunden	> 5000 **und** > 10 % der Kunden	> 50.000 **oder** > 25 % der Kunden
Ausfallzeit	> 2 Stunden	-
Wirtschaftlicher Schaden	-	> Max (0,1 % Kernkapital; 200.000 €) **oder** > 5.000.000 €
Hohe interne Eskalationsstufe	Ja	Ja, und Einstufung als Krise
Auswirkungen auf weitere Zahlungsdienstleister oder Infrastrukturen	Ja	-
Reputationsschaden	Ja	-

IT-Sicherheitsgesetz

- Zielsetzung des Gesetzes:
  - Signifikante Verbesserung der Sicherheit informationstechnischer Systeme in Deutschland
  - Schutz der IT-Systeme Kritischer Infrastrukturen und der für Infrastrukturen nötigen Netze
  - Einhaltung von Mindeststandards an IT-Sicherheit durch die Betreiber Kritischer Infrastrukturen
  - Verpflichtung der Betreiber Kritischer Infrastrukturen zum Melden von IT-Sicherheitsvorfällen an das BSI

- Es handelt sich um eine Sammlung von Änderungen, die andere Gesetze betreffen, z.B. das BSI-, Atom-, Energiewirtschafts-, Telemedien- und Telekommunikationsgesetz usw.

- Das Gesetz trat zum 24. Juli 2015 in Kraft

IT-Sicherheitsgesetz

- Betreiber **Kritischer Infrastrukturen** aus den Bereichen Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie **Finanz- und Versicherungswesen** müssen zukünftig
  - die zur Erbringung ihrer wichtigen Dienste erforderliche IT nach dem Stand der Technik angemessen absichern,
  - die Einhaltung der Absicherung regelmäßig nachweisen und
  - erhebliche IT-Sicherheitsvorfälle melden.

- Eine Rechtsverordnung definiert, welche Unternehmen als Kritische Infrastrukturen im Sinne dieses Gesetzes gelten und regelt Näheres

IT-Sicherheitsgesetz: BSI-Kritisverordnung vom 21.06.2017

Wegen ihrer besonderen Bedeutung für das Funktionieren des Gemeinwesens sind im **Sektor Finanz- und Versicherungswesen** kritische Dienstleistungen im Sinne des § 10 Absatz 1 Satz 1 des BSI-Gesetzes gemäß der Ersten Verordnung der BSI-Kritisverordnung (§ 7)

- die Bargeldversorgung,
- der kartengestützte Zahlungsverkehr
- der konventionelle Zahlungsverkehr
- die Verrechnung und die Abwicklung von Wertpapier- und Derivatgeschäften
- Versicherungsdienstleistungen

IT-Sicherheitsgesetz – Meldepflichten aus § 8a

- Betreiber Kritischer Infrastrukturen haben dem BSI **alle 2 Jahre** eine Aufstellung durchgeführter Sicherheitsaudits, Prüfungen oder Zertifizierungen **einschließlich dabei aufgedeckter Mängel** zu übermitteln. Bei Sicherheitsmängeln kann das BSI deren unverzügliche Beseitigung verlangen

- Konsequenz: Schaffung entsprechender **interner** Prozesse, die diese Meldepflicht unterstützen, einschließlich der Dokumentation der
  - internen Prozesse
  - der durchgeführten Sicherheitsaudits, Prüfungen oder Zertifizierungen
  - abgegebenen Meldungen an das BSI
  - Terminverfolgung

- Prognose: Diese Prozesse sind in das Interne Kontrollsystem zu integrieren, d.h. die interne Revision, die Verbandsrevision usw. werden auch diese Prozesse prüfen!

IT-Sicherheitsgesetz – Meldepflichten aus § 8b

- Verpflichtung zur Benennung einer Kontaktstelle, die jederzeit erreichbar ist
- Meldung von erheblichen Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastrukturen führen oder führen können
- Zusätzlich zu dieser Kontaktstelle kann eine gemeinsame, übergeordnete Ansprechstelle benannt werden (z.B. **S-CERT** für Sparkassenfinanzgruppe)
- Auch hierzu gilt: Zusätzlicher interner Aufwand durch Beschreibung und Dokumentation von entsprechenden Prozessen, Dokumentation der Bewertung von internen Vorfällen, die nicht als meldungsrelevant bewertet wurden (für Revision etc.)

Einbeziehung der Meldepflichten in bestehende Notfallbearbeitung

- Für IT-Notfälle existiert in der Haspa eine festgelegte Vorgehensweise, die in einem IT-Notfallleitfaden dokumentiert ist
  - Definition von Begriffen (z.B. Störung, IT-Notfall)
  - Festlegung von Rollen, z.B. IT-Notfallmanager, IT-Notfallteam
  - Beschreibung der Kompetenzen des IT-Notfallmanagers
  - Bereitstellung von Formularen (z.B. Lagebild, Logbuch, Protokolle usw.)

- Diese Dokumentation wurde ergänzt und erweitert um
  - Meldepflichten und -prozesse aus IT-Sicherheitsgesetz und PSD 2
  - Entscheidungshilfen für den IT-Notfallmanager, ab wann die externen Meldepflichten zu beachten sind (z.B. Schwellwerte)
  - Meldeformulare für die jeweiligen Empfänger (BSI / S-CERT oder BaFin)

- Festlegung zusätzlicher Abstimm- und Entscheidungsprozesse mit der Unternehmensleitung

Fazit (aus Sicht eines Instituts)

- Es gibt immer mehr Meldepflichten an unterschiedliche Empfänger
- Inhalte und Zielsetzungen der Meldungen sind unterschiedlich
- Meldungen von Sicherheitsaudits, Prüfungen oder Zertifizierungen sind aufwendig und erfordern wiederkehrende Prozesse einschließlich Terminüberwachung
- Institutsintern sind zusätzliche Prozesse (abgestimmt mit den beteiligten Organisationseinheiten) erforderlich
- Die internen Prozesse werden Teil des Internen Kontrollsystems
- Es entstehen zusätzliche interne Aufwände für die Dokumentation der Prozesse und der abgegebenen Meldungen
- Prüfungen (interne und externe) werden in Zukunft auch die Prozesse zu Meldepflichten an BSI und BaFin zum Gegenstand haben

Vielen Dank für Ihre Aufmerksamkeit!

Haspa
Hamburger Sparkasse

Ernst-Heinrich Paap, Dipl.-Phys.
Senior IT-Sicherheitsmanager (T.I.S.P.®)

Bereich Informationstechn.
u. Organisation
Wikingerweg 1
20537 Hamburg

Telefon 040 3579 - 9395
Telefax 040 3579 - 4066
ernst-heinrich.paap@
haspa.de