18. Juni 2020

IT-Sicherheit und –Compliance in Zeiten von Corona

Lessons Learned und Chancen für die Zukunft

Contents

Aktueller Stand: COVID-19

Auswirkungen der Corona-Pandemie auf den Regelbetrieb

Starker Anstieg von Cyber-Angriffen

Deutschland in der Corona-Pandemie eines der **häufigsten Angriffsziele**
(vgl. Kaspersky Cyberthreat Realtime Map)

Die Anzahl der Cyber-Angriffe ist während der Pandemie **um bis zu 20% gestiegen**
(vgl. Kaspersky Cyberthreat Realtime Map)

Der **Finanzsektor** wird am **häufigsten von Cyber-Angriffen getroffen**
(vgl. Fireeye Cyber Threat Map)

Explosion der Cyber-Attacken mit Corona-Bezug
(vgl. Checkpoint – Coronavirus update: In the cyber world, the graph has yet to flatten)

Behörden reagieren

Die **EZB** hat als Reaktion auf die Corona-Pandemie **Maßnahmen definiert**

Die **Aufsicht** hat unter anderem die Fristen der laufenden Verfahren verlängert und **vertagt Termine**

Das **BBK und BSI** hat **Handlungsempfehlungen für** Betreiber Kritischer Infrastrukturen für **Covid-19** veröffentlicht

Auswirkungen auf Technologien

Der **Datenverkehr** bei Internet- und Telefonnutzung **hat zugenommen** und erhöht Last auf Telekommunikationsnetze
(vgl. CEO Vodafone Germany – Corona und die Stunde der Netzbetreiber)

Ansturm auf digitale Lösungen zur Zusammenarbeit: Microsoft Teams bspw. konnte in nur einer Woche **zwölf Millionen neue Nutzer** gewinnen
(vgl. CEO Vodafone Germany – Corona und die Stunde der Netzbetreiber)

Home Office erschwert Regelbetrieb

Ein Großteil der Angestellten arbeitet aufgrund von Corona **von zu Hause** aus
(vgl. WiWo – Krieg der Konferenzsysteme)

Lieferverzögerungen durch hohe Nachfrage nach Ausstattung für **Home Office-Lösungen**
(vgl. Spiegel – Nachfrageboom bei PCs, Notebooks)

Herausforderungen für die IT-Sicherheit und -Compliance

Welche Themen Kapitelverwaltungsgesellschaften beachten müssen

Basierend auf unseren umfangreichen Erfahrungen aus der Vorbereitung, Begleitung und Nachbereitung von aufsichtsrechtlichen Prüfungen, Marktbeobachtungen und Gespräche mit Unternehmen aus dem Finanzsektor haben wir fünf Handlungsfelder identifiziert:

Notfallplanung

Eine getestete und kommunizierte **Notfall-planung**, unter Berück-sichtigung der **relevanten Ausfallszenarien** und der **Kritikalität** der **Geschäftsprozesse** als Grundlage für die Notfallbewältigung.

Digitalisierung von Geschäftsprozessen

Digitale Tools und **Lösungen**, welche die Durchführung von Geschäftsprozessen und Kontrollen im „new normal“ ermöglichen bzw. deren Ablauf sogar optimieren.

Chancen und Risiken der Home Office Nutzung

Aus der Arbeit im **Home Office** entstehen **Chancen** aber auch **Risiken** – hier gilt es, durch entsprechen-de Regelungen und Vor-gaben ein **Mindestmaß an Sicherheit** zu gewähr-leisten.

Informations-sicherheitsfunktion

Der **Informations-sicherheitsbeauftragte** als zentrale Einheit für die Informationssicherheit erstellt **Vorgaben**, definiert Prozesse und **überwacht** deren **Umsetzung**.

Cloud Services

Die **Nutzung** von **Cloud Services** als eine sichere und kosteneffiziente Mög-lichkeit für den **ortsunab-hängigen Zugriff** auf die erforderliche **IT-Archi-tektur** durch die Mitarbeiter.

Notfallplanung

Die aktuelle Marktlage

Wie ist die Notfallplanung des Finanzsektors hinsichtlich Pandemien aufgestellt?

Aktuelle Situation und Herausforderungen

Pandemiepläne

Ein Großteil der Unternehmen **besitzt Pandemiepläne**.

Die Pandemiepläne fokussieren sich auf den **Ausfall von IT**, **Personalausfall** wird **nicht** bzw. **nicht ausreichend behandelt**.

Outsourcing

Dienstleister und erbrachte **Services** werden **grundsätzlich überwacht**.

Der Ernstfall einer **Pandemie** wurde in den **wenigsten** Fällen bei den Dienstleistern auf den **Prüfstand gestellt**.

Medizinische Ausstattung

Eine grundsätzliche **medizinische Ausstattung** ist **gegeben**.

Bei einer Pandemie kommt die **medizinische Ausstattung** von Unternehmen schnell an **ihre Grenzen**.

Reaktion der Aufsicht

Welche Maßnahmen verlangt die Aufsicht konkret?

- Festlegung, Umsetzung und Aufrechterhaltung einer **angemessenen Notfallplanung**
- Gewährleistung des **Erhalts wesentlicher Systeme** und **Verfahren** im Falle einer Störung

Welche Anforderungen lassen sich aus der Prüfungspraxis ableiten?

- Kontinuitätsstrategien für das **Szenario Pandemie**
- **Funktionsfähige Kontinuitätsstrategien** für die Dauer der Pandemie
- **Bereitstellung** erforderlicher **IT-Kapazitäten**
- **Schutz** der **Kontinuitätsstrategien** vor Cyber Threats
- **Absicherung kritischer Dienstleister** für die Pandemie

Befragung durch die BaFin

Die BaFin hat eine Befragung hinsichtlich der durch die beaufsichtigten Institute **ergriffenen Maßnahmen** durchgeführt. Dies erfolgt auf Basis der durch die EZB veröffentlichten Vorgaben vom 3. März 2020.

Erfolgsfaktoren des Business Continuity Managements

Was können Kapitelverwaltungsgesellschaften tun, um Auswirkungen eines Notfalls zu verringern?

Notfallvorsorge

- Erstellung und Kommunikation skalierbarer **Kontinuitätsstrategien,** insb. auch für den Fall einer Pandemie
- Beschaffung und Bereitstellung von angemessenem **IT-Equipment** für die User, die “work from anywhere” ermöglichen
- Schaffung von **Kommunikations-** und **Informationskanälen** (bspw. Einrichten einer Notfallkontaktstelle)
- Abstimmung und Test der Notfallplanungen mit **Dienstleistern**
- Etablierung von Prozessen zur Beschaffung von Medizin und **Hygieneartikeln**

Notfallbewältigung

- Ermöglichung von **Home Office Lösungen** zur Aufrechterhaltung der wesentlichen Geschäftsprozesse und des Geschäftsbetriebs
- Sicherstellung der Dienstleistungen durch vertraglich vereinbarte **Notfallmaßnahmen**
- Medizinische Vor-Ort-Maßnahmen (bspw. Bereitstellung von **Desinfektionsstationen** vor Kantinen oder sanitären Anlagen)

Lessons Learned

- Einleitung der vorab definierten Maßnahmen zur **Wiederaufnahme** des **Normalbetriebs**
- Zentralisierte **Unterrichtung** der deaktivierten Beschäftigten über Wiederaufnahme des Normalbetriebs
- **Lessons Learned** aus dem Notfall **ableiten** und bestehende Verfahren optimieren, insbesondere im Bereich der **Notfallplanung** und der **Informationssicherheit**

Digitalisierung von Geschäftsprozessen

Einführung digitaler Lösungen

Welche Ansatzpunkte gibt es zur Digitalisierung von Prozessen?

Status quo

- Die Ausnahmesituation der Corona-Pandemie ist bewältigt und es entwickelt sich ein „*new normal*“.
- Im Regelbetrieb ergeben sich Möglichkeiten zur Optimierung von Prozessen und Kontrollen.

Auswahl

- Welche Prozesse und Kontrollen eignen sich für die Optimierung durch Einführung digitaler Lösungen? Oder ergaben sich Probleme?
- Beispiel: bisher auf Papier dokumentierte Kontrollen im 4-Augen-Prinzip

Implementierung

- Welche Lösungen sind erforderlich zur Optimierung des Prozesses oder der Kontrolle?
- Beispiel: Einführung digitaler Signaturen

Anforderungen der KAIT

Die **Vorgaben** der **KAIT** hinsichtlich der **Erfassung** des **Informationsverbunds** (insb. Tz. 19) und der **Ermittlung** des **Schutzbedarfs** und dazugehöriger Sollmaßnahmen (insb. Tz. 20 und 21) können als Grundlage für solch eine Priorisierung dienen.

Abgleich der Lösungsansätze mit **Sicherheitsrichtlinien** innerhalb der Organisation

Einhaltung geltender Gesetze (z.B. Datenschutz) und vertraglicher Regelungen zur Cyber Security (z.B. Kundenverträge)

Berücksichtigung von Sicherheitsstandards bei der Beschaffung von Lösungen

Auch hinsichtlich der Konformität mit entsprechenden Sicherheitsvorgaben und –standards sind in der KAIT bereits Vorgaben enthalten, bspw. zur **Ausrichtung** an **gängigen Standards** (Tz. 2), zur **Erstellung** von **Sicherheitsrichtlinien** (Tz. 26) und zur **Überprüfung** derer durch den **Informationssicherheitsbeauftragten** (Tz. 27).

Chancen und Risiken der Home Office Nutzung

Umsetzung von Home Office-Lösungen

Wie kann eine angemessene Sicherheit aufrecht erhalten werden?

Chancen

Die Umsetzung von Home Office Lösungen bietet Mitarbeitern viele Möglichkeiten, bspw. im Hinblick der Work-Life-Balance und einer flexibleren Gestaltung der Arbeitszeit und des Arbeitsortes. Gleichwohl gilt es hierbei, ein Mindestmaß an Sicherheit zu gewährleisten und die Maßnahmen zur Informationssicherheit auch auf die spezielle Risiken im Home Office auszurichten.

Beispielhafte Risiken durch Einsatz von Home Office		Beispielhafte Maßnahmen zur Informationssicherheit
Unbefugte Einsicht in sensible Daten	Durch **fehlerhafte Verräumung oder Entsorgung** sensibler Daten im Home Office können unbefugte Dritte Einsicht in diese erhalten.	Definition und Kommunikation klarer Regelungen bzw. Vorgaben zum Arbeiten aus dem Home Office
Angriffsziel Remote-Zugänge	Angreifer versuchen durch **Phishing Mails**, die aktuelle Situation auszunutzen und Authentifizierungsdaten der Remote-Zugänge abzugreifen.	Etablieren von Prozessen zur sicheren Entsorgung sensibler Daten von zu Hause
Manipulation von Übertragungs-protokollen	Werden zur Kommunikation zwischen dem Remote-Arbeitsplatz und dem Firmennetz unverschlüsselte **Protokolle** verwendet, können Angreifer diese **abhören oder manipulieren.**	Awareness hinsichtlich der Identifikation und Verfahren zur Behandlung von Phishing Mails etablieren Einrichtung sicherer Kommunikationskanäle zum Zugriff auf das Firmennetz (bspw. über ein kryptographisch abgesichertes VPN)

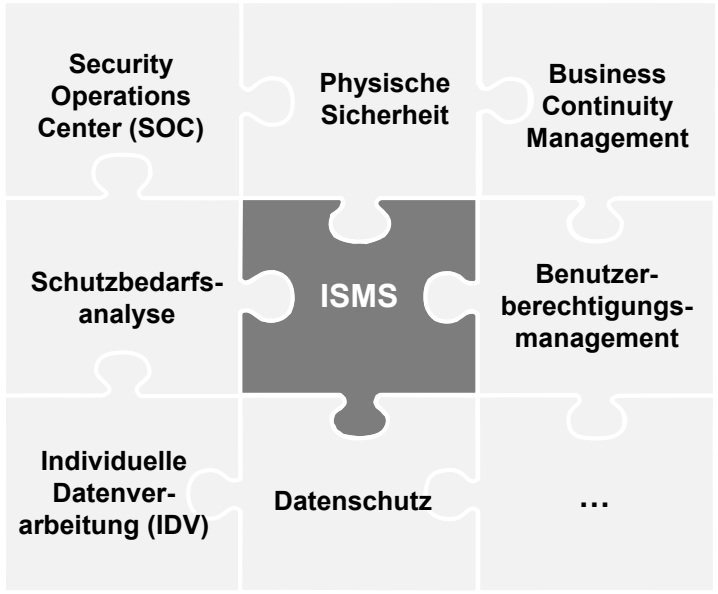
Die Anforderungen der KAIT (insb. an das Informationssicher-heitsmanagement-Kapitel II.4) betreffen auch etwaige Home Office Lösungen und Prozesse.

Informationssicherheits-funktion und -vorgaben

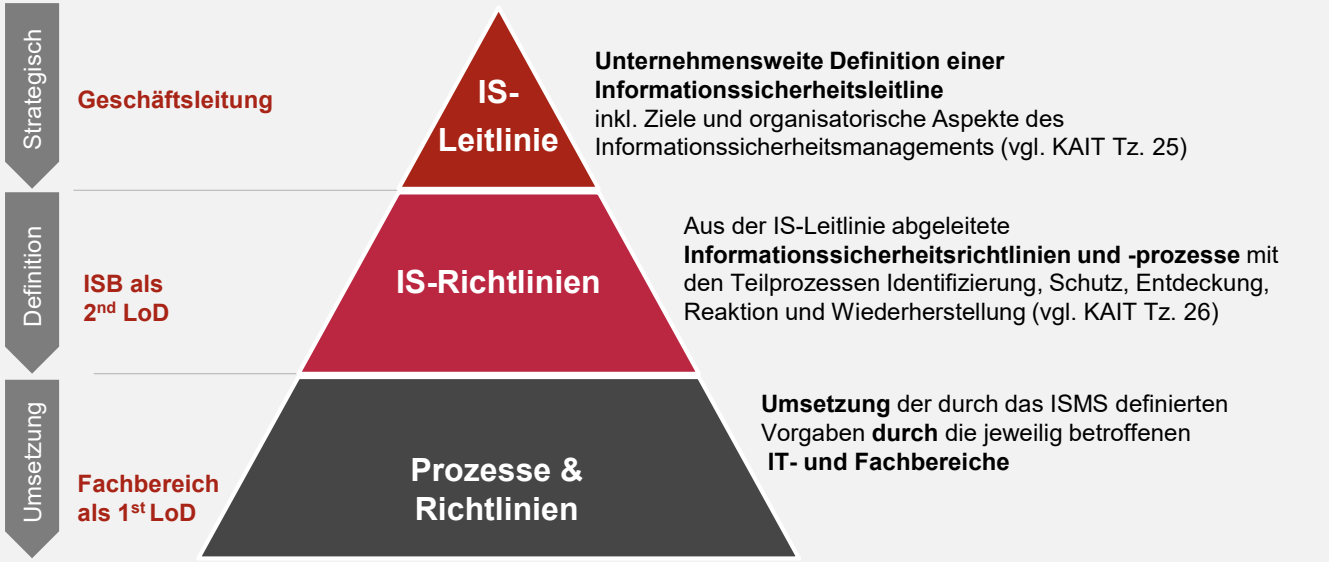
Informationssicherheitsfunktion und -vorgaben

Zentrale Einheit zur Erstellung von Vorgaben und Prozessen im Bereich der Informationssicherheit

ISMS als Querschnittsfunktion…



…mit einer aufeinander aufbauenden Dokumentenpyramide



Anforderungen der KAIT

Die **Vorgaben** der **KAIT** umfassen insb. die **Ziele** und organisatorischen Aspekte des **Informations-sicherheitsmanagements** (vgl. KAIT Tz. 25) sowie die **Erstellung** von **IS-Richtlinien** und –**Prozessen** mit den Teilprozessen Identifizierung, Schutz, Entdeckung, Reaktion und Wiederherstellung (vgl. KAIT Tz. 26)

Auch bei der **Einführung** von bspw. Technologien und Prozessen für **Home Office Lösungen** hat eine entsprechende **Erweiterung** und **Berücksichtigung** in der schriftlich fixierten Ordnung des ISMS zu erfolgen. Dabei ist auf eine entsprechende Ableitung und Konsistenz zwischen den Ebenen der Dokumentenpyramide zu achten.

Stärkere Nutzung von Cloud Services

Nutzung von Cloud Services

Vorteile für Unternehmen im AWM-Sektor

Veränderung

Bewegung im Finanzsektor

- Rasantes **Wachstum** beim **Angebot** von **Cloud Services** ermöglicht neue Modelle für das Zusammenspiel von IT und Fachbereich
- Cloud Services **sprechen** die **Bedürfnisse** vieler Kunden im Finanzsektor **an** – u.a. durch Kosteneffizienz und die schnelle Ermöglichung neuer Services
- Banken und Finanzdienstleister nutzen **große Datensammlungen** um sich gegenüber der Konkurrenz abzuheben und benötigen für die **Analyse** dieser die erforderlichen Rechenkapazitäten

Beobachtung

Nutzung von Cloud-Services im AWM-Bereich

Aus Gesprächen und gemäß unserer Erfahrungen aus durchgeführten Projekten und Prüfungen schätzen wir den Umsetzungsstand folgendermaßen ein:

- Ein Großteil der KVGen plant die **strategische Nutzung** von Cloud Services in Geschäftsprozessen
- Ein Teil hiervon hat die geplante **Nutzung** auch bereits entsprechend **dokumentiert**, bspw. in einer **IT-Strategie**
- KVGen arbeiten aktuell insbesondere an der **Konzeption konkreter Anwendungsfälle** – eine Umsetzung und **produktive Nutzung** von Cloud Services in Geschäftsprozessen erfolgt bisher in den **wenigsten Fällen**

Anforderungen

Regulatorische Anforderungen

Auch bei der Nutzung von Cloud Services gilt es, die entsprechenden **regulatorischen Anforderungen** zu beachten:

- KAMaRisk AT 10 mit Anforderungen an die Klassifikation und die Steuerung und Überwachung von Auslagerungen
- KAIT II.8 zum sonstigen Fremdbezug von IT-Dienstleistungen

Darüber hinaus sind auch die aus der Nutzung von Cloud Services entstehenden **Risiken** (bspw. Lokation und Zugriff auf Daten) entsprechend **zu managen**.

Neue Guidelines der ESMA bzgl. der **Auslagerung** an **Cloud Provider** wurden Anfang Juni zur Konsultation gestellt

Ihre Ansprechpartner

Marc Billeb
WP, StB, CISA
Partner Assurance

Tel. +49 69 9585-2723
Mobil +49 175 7256447

marc.billeb@pwc.com

Alexandra Naumann
CISA
Senior Managerin Assurance

Tel. +49 69 9585-1841
Mobil +49 170 7601590

alexandra.naumann@pwc.com

Vielen Dank für Ihre Aufmerksamkeit.

pwc.de