KRITIS: BCM und Business Resilienz für kritische Dienstleistungen

Dieses Grundlagendokument vermittelt eine Übersicht der gesetzlichen Anforderungen und Prüfungsgrundlagen im Rahmen von KRITIS. Kritische Infrastrukturen erbringen Dienstleistungen, die maßgeblich zur Versorgung der Bevölkerung beitragen. Somit ist im Sinne der allgemeinen Resilienz deren Kontinuität durch die Einrichtung eines Business Continuity Management Systems zu sichern. Anhand der Erfahrungen aus den KRITIS-Prüfungen, aus der der Sicht der Prüfer, werden die Mindestmaßnahmen und die ersten Arbeitsschritte im Business Continuity Management erläutert.

Überblick: KRITIS

In Zeiten der zunehmenden Digitalisierung unserer Gesellschaft eröffnen sich immer weitere Angriffsflächen. Während Diebe vor Jahren noch Banken überfallen mussten um an Geld heranzukommen, reicht heute ein Überfall auf die IT-Infrastruktur, um an Geld heranzukommen, reicht heute ein Überfall auf die IT-Infrastruktur, um anschließend das Geld bequem am Geldautomaten abzuheben.

Immer neuere Cyber-Angriffe führen dazu, dass diese für Unternehmen nicht mehr als Ausnahme, sondern als Regel angesehen werden. Laut aktuellen Studien sind etwa 45% der Unternehmen regelmäßig Opfer von Cyber-Angriffen.

Auf die Sicherheit der Infrastrukturen sollte ein besonderes Augenmerk gelegt werden. Durch das IT-Sicherheitsgesetz und den § 8a BSIG wurden hierfür die Weichen gestellt. Das IT-Sicherheitsgesetz bildet hierbei die nationale Umsetzung der europäischen Richtlinie (Richtlinie (EU) 2016/1148) ab. Durch das BSIG hat das BSI weitreichende Rechte und Pflichten erhalten, um den Schutz von kritischen Infrastrukturen in Deutschland zu gewährleisten.

Im Rahmen der BSI-Kritisverordnung (KritisV) wurden zwei Körbe definiert, welche den verschiedenen KRITIS-Sektoren angehören. Sie teilen sich in die regulierten Sektoren und nicht regulierten Sektoren. Zu den regulierten Sektoren zählen Energie, IT und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen, Staat und Verwaltung sowie Medien und Kultur. Nicht alle Sektoren werden direkt durch das BSI überwacht. Die Bereiche Energie sowie IT und Telekommunikation werden durch die Bundesnetzagentur betreut. Die Bereiche Staat und Verwaltung sowie Medien und Kultur fallen nicht direkt unter die KritisV und werden separat betreut.

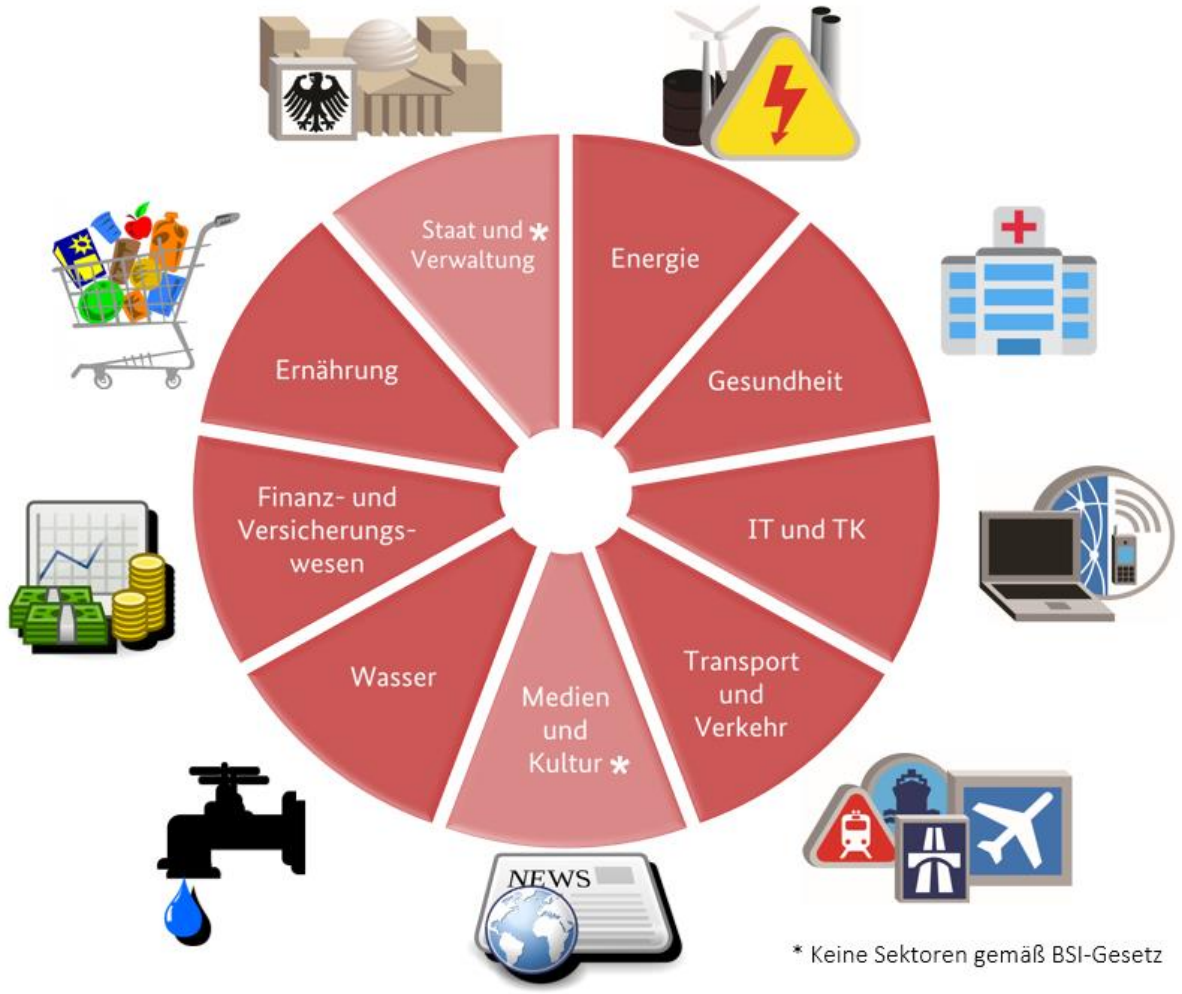

Abbildung 1: KRITIS-Sektoren im Überblick

Die Prüfung, ob ein Betrieb unter die BSI-Kritisverordnung fällt, muss der Betreiber selbstständig anhand des Gesetzes durchführen. In der KritisV unter Anhang 6 wird beispielsweise definiert, dass das Autorisierungssystem einer Bank eine kritische Dienstleistung (kDL) darstellt, sofern es mehr als 15 Millionen Transaktionen pro Jahr durchführt.

Anforderungen gemäß KRITIS an die Betreiber

Geprüft werden IT-gestützte Anlagen, mit denen kritische Dienstleistungen erbracht werden. Überschreiten die Anlagen die in der BSI-Kritisverordnung aufgeführten Schwellenwerte, handelt es sich um Kritische Infrastrukturen gemäß § 8a BSIG. In diesem Fall hat der Betreiber dafür Sorge zu tragen, dass die Anlagen mit angemessenen Sicherheitsmaßnahmen nach dem „Stand der Technik“ abgesichert werden. Im Rahmen von KRITIS werden unter dem „Stand der Technik“ Normen und Branchenstandards oder auch vergleichbare Verfahren, Einrichtungen und Betriebsweisen verstanden, welche bereits mit Erfolg in der Praxis erprobt wurden.

Im Gegensatz zu den etablierten Risikomanagementsystemen gilt für die Absicherung der Kritischen Infrastrukturen eine Einschränkung bezüglich der Behandlung von Risiken. Der Fokus bei KRITIS liegt auf der Verfügbarkeit der betroffenen Anlagen. Die Anforderungen dienen primär dem Schutz der Bevölkerung und nur nachgelagert dem Schutz der Unternehmen. Damit sind Risikostrategien wie Risikotransfer oder Risikoakzeptanz, welche einen Ausfall prinzipiell erlauben würden, nicht zugelassen. So stellt eine Versicherung als Risikomaßnahme kein angemessenes Werkzeug zur Vermeidung von Versorgungsengpässen dar.

Hinzu kommt, dass für die Absicherung der IT nicht nur reine IT-Risiken, wie zum Beispiel Cyber-Angriffe, betrachtet werden sollen. Auslöser für informationstechnische Störungen können auch physische Bedrohungen sein, weshalb der All-Gefahrenansatz bei der Risikobetrachtung gefordert wird. Das bedeutet, dass alle relevanten Bedrohungen und Schwachstellen der IT-Systeme, Komponenten und Prozesse, die zur Erbringung einer kritischen Dienstleistung notwendig sind, behandelt werden müssen.

Die für Kritische Infrastrukturen relevanten Bedrohungs- und Schwachstellenkategorien werden im Anhang der „Orientierungshilfe zu Inhalten und Anforderungen an Branchenspezifische Sicherheitsstandards (B3S) gemäß § 8a (2) BSIG“ (Orientierungshilfe B3S) aufgeführt. Alternativ zu diesen können für die Erfüllung des All-Gefahrenansatzes auch die elementaren Gefährdungen des BSI IT-Grundschutzes verwendet werden.

Pflicht zur Nachweiserbringung

Die Betreiber Kritischer Infrastrukturen sind gemäß § 8a BSIG Absatz 1 verpflichtet, mindestens alle zwei Jahre die Erfüllung der Anforderungen nachzuweisen. Die Nachweise sind basierend auf einer geeigneten Prüfungsgrundlage zu erstellen und können durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen.

Ausnahmen für diese Pflicht stellen die Betreiber von öffentlichen Telekommunikationsnetzen dar, welche durch die Bundesnetzagentur alle zwei Jahre geprüft werden. Auch Betreiber von Energieversorgungsnetzen und Energieanlagen unterliegen bereits speziellen Anforderungen nach § 11 EnWG und fallen somit nicht unter die Nachweispflicht für KRITIS-Betreiber.

Mögliche Zusammensetzung einer Prüfungsgrundlage

Zur Vorbereitung der Prüfung gemäß § 8a BSIG wird eine geeignete Prüfungsgrundlage erstellt, um Art und Umfang zu festgelegt. Die Prüfgrundlage wird vorab zwischen den Betreibern und der prüfenden Stelle abgestimmt. Die Prüfungsgrundlage soll den „Stand der Technik“ widerspiegeln und organisatorische sowie technische Vorgaben enthalten. Weiterhin sollte die Grundlage „prüfbar“ sein, indem sie zum Beispiel einem etablierten Standard entspricht. Hierbei lässt sie sich typischerweise in einen allgemeinen Teil zum Informationssicherheitsmanagement (ISMS) und einen branchenspezifischen Teil

gliedern. Für die Prüfung nach § 8a BSIG hat sich dieses Vorgehen auch in der Praxis als zweckmäßig erwiesen.

Die Prüfungsgrundlage kann individuell zusammengestellt werden. So kann zum Beispiel eine bestehende Umsetzung der ISO 27001 auf der Basis von IT-Grundschutz sowie die Umsetzung von branchenspezifischen und technischen Standards als Grundlage dienen. Da für den branchenspezifischen Teil nicht immer einheitliche Standards vorhanden oder diese aus anderen Gründen nicht praktikabel sind, gibt es noch eine andere Möglichkeit, diesen Teil der Prüfungsgrundlage zu erfüllen. Entsprechend § 8a Absatz 2 BSIG gibt es die Möglichkeit, für die KRITIS-Prüfung Branchenspezifische Sicherheitsstandards (B3S) zu nutzen. Diese können von Branchenverbänden erstellt und von den betreffenden Betreibern als Teil einer Prüfgrundlage genutzt werden.

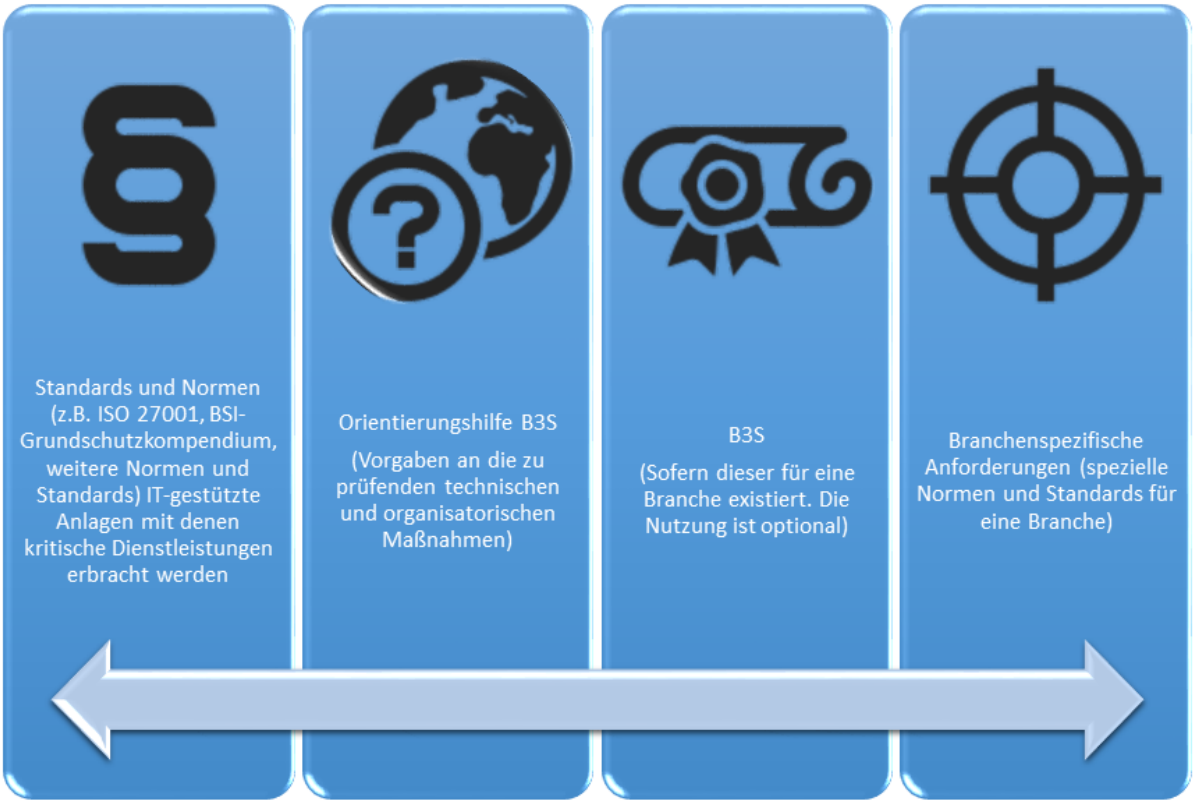

Abbildung 2: Mögliche Bausteine einer Prüfungsgrundlage

Business Continuity innerhalb der KRITIS-Prüfung

Ungeachtet der Zusammenstellung der Prüfgrundlage ist das Business Continuity Management (BCM) ein wichtiger Baustein und Prüfungsthema innerhalb der KRITIS-Prüfungen. Andere Bausteine, die in erster Linie dem Schutz der kritischen Dienstleistung dienen, sind zum Beispiel Anforderungen an das Informationssicherheitsmanagementsystem (ISMS) und die technische Sicherheit. Die Anforderungen an das Business Continuity Management decken die Aspekte ab, die die Aufrechterhaltung der kritischen Dienstleistung nach einem Vorfall gewährleisten. Ziele

und Scope eines regulären Business Continuity Management Systems (BCMS) unterscheiden sich dabei von denen eines BCMS, welches sich auf die kritische Dienstleistung fokussiert.

In einem regulären BCMS legt die Geschäftsführung anhand ihres Risikoappetits fest, wie viel Resilienz bzw. Kontinuität sie dem Unternehmen zugesteht. Hierzu fließen Anforderungen von Interessengruppen (Kunden, Geschäftspartner etc.) sowie gesetzliche Anforderungen ein. Im Fokus des BCM stehen alle zeitkritischen Geschäftsprozesse, die im Rahmen der Business Impact Analyse (BIA) erhoben werden. Ein Prozess gilt als zeitkritisch, wenn bei dessen Ausfall bis zu einem definierten Zeitpunkt (bspw. innerhalb von vier Wochen) mit nicht tolerierbaren Auswirkungen auf die Institution zu rechnen ist. Nicht tolerierbare Auswirkungen können finanzielle Verluste, Imageschäden, vertragliche/ gesetzliche Verstöße oder die Beeinträchtigung der körperlichen Unversehrtheit sein. Was als tolerabel angesehen wird, kann von der Größe, Art oder Auftrag der Institution unterschiedlich sein und wird daher individuell durch das Management der Institution festgelegt. Während ein Unternehmen bei einem Verlust von einer Million pro Tag insolvent geht, kann ein anderes diese Komplikation ohne Schwierigkeiten hinnehmen, ohne den Notfall auszurufen. Entsprechend kann je nach Risikoappetit der Institution der Fokus auf reaktive Maßnahmen gelegt werden, die erst bei Eintritt eines Notfalls zum Einsatz kommen.

Ein BCMS nach KRITIS legt den Fokus auf Resilienz. Hierbei soll durch präventive Maßnahmen ein Ausfall ausgeschlossen werden. Sollte es doch zu einem Ausfall kommen, soll der Wiederanlauf der kritischen Dienstleistung möglichst schnell sichergestellt werden. Anhand von Workarounds, die in den Business Continuity Plänen (BCP) beschrieben werden, soll zudem ein Notbetrieb ermöglicht werden, der einen „minimum output“ liefert. Im Fokus stehen damit alle Prozesse, die die Erbringung der kritischen Dienstleistung sicherstellen oder wesentlich zu dessen Erbringung beitragen, wie zum Beispiel notwendige Unterstützungsprozesse. Somit ist auch die Frage nach den nicht tolerierbaren Auswirkungen eine andere. Für KRITIS ist es irrelevant, ob finanzielle Auswirkungen oder Imageverluste zu erwarten sind. Entscheidend ist die Frage, ob die Versorgung der kDL aufrechterhalten werden kann. Entsprechend spielt auch das Risikoakzeptanzniveau der Institution eine untergeordnete Rolle. Bedeutender ist: Wie lange kann der Ausfall der kDL den Leistungsbeziehern abverlangt werden? Dabei entspricht der Zeithorizont eher Stunden oder Tagen als Wochen. Somit wird in einer BIA vornehmlich nur eine Schadenskategorie betrachtet, statt der üblichen drei bis vier oben genannten. Die gewählten Kontinuitätsstrategien und -lösungen zielen darauf ab, die kDL für die Leistungsbezieher sicherzustellen, statt Schaden von der Institution abzuwenden.

KRITIS BCM		Normales BCM
• Kunden-/Bevölkerungssicht	Strategie	• Interessensgruppen
• Nur Prozesse für die kDL inkl. Unterstützungsprozesse • Wichtigste Schadenskategorie: Versorgungssicherheit	BIA	• Alle Geschäftsprozesse • Mehrere Schadenskategorien
• Nur Prozesse für die kDL inkl. Unterstützungsprozesse	BCP	• Alle kritischen Geschäftsprozesse
• Nur Prozesse für die kDL inkl. Unterstützungsprozesse	Übungen und Tests	• Alle kritischen Geschäftsprozesse

Abbildung 3: Unterschiede zwischen KRITIS BCM und einem normalen BCM

Mindestmaßnahmen an das Business Continuity Management

Im Rahmen der KRITIS-Prüfung wird kein vollumfängliches Business Continuity Management gefordert, auch wenn dieses in jedem Falle empfehlenswert ist. Nachfolgend werden die vom BSI geforderten Mindestmaßnahmen, basierend auf der Orientierungshilfe B3S und dem Prüfer-Erfahrungsaustausch mit dem BSI, beschrieben.

Das BSI empfiehlt, das Business Continuity Management oder auch Notfallmanagement nach einem der gängigen Standards auszurichten z.B. BSI-Standard 100-4 oder ISO 22301 (Social Security - Business Continuity Management Systems – Requirements) und ISO 22313 (Social Security - Business Continuity Management Systems – Guidance). Dies garantiert einen strukturierten Aufbau und Umsetzung des Managementsystems.
Die Standards folgen einem Lebenszyklusmodell, dem PDCA-Zyklus (Plan-Do-Check-Act), bei dem in wiederkehrender Reihenfolge die einzelnen Phasen durchlaufen werden. Das Business Continuity Management sollte nach dem PDCA-Zyklus ausgerichtet sein, um eine stetige Verbesserung des Managementsystems und der Prozesse zu gewährleisten. Die nachfolgende Grafik zeigt den Aufbau des PDCA-Zyklus.

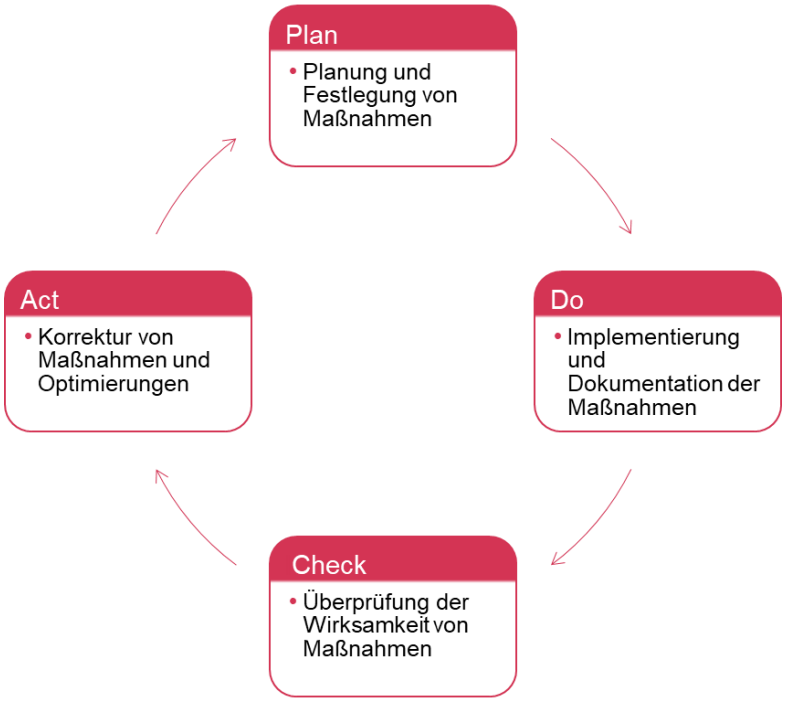

Abbildung 4: Plan-Do-Check-Act-Zyklus

In der ersten Phase (Plan) findet die Planung und Festlegung von Maßnahmen statt. Für das Business Continuity Management heißt das konkret, eine Richtlinie oder Policy zu verfassen, die das Managementsystem und die Schutzziele beschreiben sowie das Commitment des Managements beinhaltet.
In der zweiten Phase (Do) findet die Implementierung und Dokumentation statt. Hier wird die Business Impact Analyse und die Risikoanalyse durchgeführt sowie Handlungsoptionen für die Continuity Pläne festgelegt. Klassischerweise beinhaltet diese Phase ebenso das Notfallmanagement für das Outsourcing und die Awareness und Schulungen der Mitarbeiter, doch diese zwei Themenblöcke werden nicht gezielt in der Prüfung abgefragt. Das Thema Outsourcing wird teilweise im Risikomanagement betrachtet und die Themen Awareness und Schulungen könnten auch mit den durchgeführten Übungen und Tests subsumiert werden, falls der KRITIS-Betreiber keine expliziten Awareness-Maßnahmen oder Schulungen nachweisen kann.
In der dritten Phase (Check) werden die Übungen und Tests durchgeführt. Die sich daraus ergebenden Maßnahmen und gewonnenen Erkenntnisse (Lessons Learned) werden dokumentiert.
In der letzten Phase (Act) werden anhand der Ergebnisse der Übungen und Tests eventuelle Anpassungen in der Dokumentation, in Verfahren oder in Prozessen vorgenommen. Idealerweise wird dieser PDCA-Zyklus innerhalb eines Jahres vollständig durchlaufen.

In den nachfolgenden Abschnitten werden einzelne Bestandteile des PDCA Zyklus näher beleuchtet:

- PLAN: Business Impact Analyse
- DO: Business Continuity Pläne

- CHECK: Übungen und Tests
- ACT: Ergebnisse/Maßnahmen aus Übungen und Tests

Business Impact Analyse

Die Grundlage des gesamten Business Continuity Managements bildet die Business Impact Analyse (BIA). In der BIA werden die Geschäftsprozesse gemäß ihrer Kritikalität im Zeitablauf eingestuft. Diese Einstufung sollte immer nach einem einheitlichen Schema ablaufen, um die Vergleichbarkeit und damit eine hohe Qualität der Ergebnisse sicherzustellen. Zusätzlich werden die Abhängigkeiten der Geschäftsprozesse untereinander erfasst sowie die geschäftskritischen Faktoren und benötigten Ressourcen (z.B. Personal, IT, Dienstleister, Ausweicharbeitsplätze etc.) für den Notfall zugeordnet.

Die Erfahrungen aus der Prüfung zeigen, dass grundsätzlich auch eine vereinfachte Variante der BIA ausreicht. Wichtig ist, dass die kDL erkannt und bewertet sowie die kritischen Ressourcen identifiziert werden. Die Mindestanforderung des BSI ist, dass die Single Points of Failure (idealerweise innerhalb der BIA) erfasst werden. Die Single Points of Failure beschreiben Komponenten, deren Nichtverfügbarkeit den Ausfall der gesamten Anlagen bzw. des gesamten Geschäftsprozesses auslösen kann. Diese sind zu erfassen, zu bewerten und gegebenenfalls zu eliminieren.

Business Continuity Pläne

Um auf Notfälle oder Unterbrechungen reagieren zu können, wird für alle kDL und deren kritischen Ressourcen ein Business Continuity Plan benötigt. Dieser beschreibt die einzelnen Handlungsanweisungen bei einem Ausfall einer oder mehrerer Ressourcen, die zu einer Unterbrechung der kDL führen könnten. Das oberste Ziel ist immer, die ununterbrochene Gewährleistung der Versorgungssicherheit der Bevölkerung.

Nachdem in der BIA die kDL und die dazugehörigen Ressourcen identifiziert wurden, können die Business Continuity Pläne geschrieben werden. Im Business Continuity Plan werden Kontinuitätsstrategien definiert, für die BCM-Ausfalltypen Gebäude, Personal, IT und Dienstleister. Diese Kontinuitätsstrategien müssen zuvor zentral ausgewählt und bewertet werden. Kontinuitätsstrategien für den Ausfalltyp Gebäude könnten folgende sein: Nutzung der Ausweicharbeitsplätze (auch im Schichtbetrieb), ausgestatteter mobiler Arbeitsplatz, Übernahme durch Mitarbeiter an anderen Standorten oder Outsourcing. Es muss einzeln bewertet werden, ob jegliche Option eine Kontinuitätsstrategie für den kDL-Betreiber darstellt. Diese alternativen Abläufe sind anschließend in einem Business Continuity Plan zu verschriftlichen. Ferner sind die Rahmenbedingungen für die im Business Continuity Plan aufgeführten alternativen Abläufe in Form von Notfallvorsorgemaßnahmen zu implementieren.

Übungen und Tests

Um die Leistungsfähigkeit und Wirksamkeit der Daten der BIA, der Business Continuity Pläne und der umgesetzten Vorsorgemaßnahmen einzuschätzen, werden Übungen und Tests unterschiedlicher Kategorie durchgeführt, ausgewertet und protokolliert. Die Tests sollten unter der Einbindung des IT Service Continuity Management (ITSCM) durchgeführt werden, da in der Regel kDL mit IT-Anwendungen verbunden sind. Das BSI empfiehlt, die Vorgehensweise zur Bewältigung seltener oder besonders folgenreicher Ereignisse zu üben. Dies kann beispielsweise durch interne Übungen und Tests, Übungen mit externen Partnern (insbesondere aus dem Kontext der kDL), Übungen im Rahmen des Notfallmanagements, Kommunikationsübungen, Planübungen, Krisenübungen oder ein Training seltener Ereignisse erfolgen. Das BCM führt Prozesstests und Notfall- oder Krisenstabsübungen durch. Das ITSCM beübt die Wiederanlauf- und Wiederherstellungspläne und das BCM die Business Continuity Pläne und die Notfall- und Krisenorganisation. Um eine Übungsmüdigkeit zu vermeiden, sollten regelmäßig andere Ausfallszenarien getestet werden.

Die Erfahrungen bei Prüfungen zeigen, dass der Fokus auf der Überprüfung von Übungs- und Testumsetzung sowie der Testplanung liegt. Dadurch wird ersichtlich, ob es sich um einen gelebten Prozess handelt. Ebenfalls werden die Übungs- und Testergebnisse auf ihre Vollständigkeit und den daraus abgeleiteten Maßnahmen und Lessons Learned angeschaut.

Tipp: Falls echte Vorfälle entsprechend dokumentiert wurden, können diese als "Tests" für die Prüfung fungieren.

Schnittstellenmanagement

Im Business Continuity Management müssen die Schnittstellen zu anderen Managementsystemen oder Stakeholdern betrachtet werden. Es bestehen Schnittstellen hinsichtlich Abstimmung und Planung von Übungen und Tests, Risikoanalysen, internen Audits sowie Schulungen und Sensibilisierung. Zu einigen Schnittstellen muss ein direkter Informationsfluss aufgebaut werden z.B. ITSCM, IT-Sicherheit oder Kommunikation. Das ITSCM benötigt beispielweise die erhobenen Anforderungen aus der BIA an einzelne IT-Anwendungen in Form von RTO und RPO (Recovery Time Objective und Recovery Point Objective), um diese mit den technischen Möglichkeiten der IT abzustimmen.

Mindestmaßnahmen auf einen Blick

Zu den Mindestmaßnahmen des Business Continuity Management gehören:

- Durchführung der Business Impact Analyse
- Identifikation der Single Points of Failure
- Entwicklung von Kontinuitäts- und Wiederanlaufstrategien

- Erstellung von Business Continuity Plänen
- Sicherstellung der geeigneten Verzahnung mit der IT-Sicherheit
- Übungen und Tests
    - interne Übungen und Systemtests
    - Übungen mit externen Partnern
    - Übungen des Notfall- und Krisenmanagements (Kommunikationsübungen, Krisenstabsübung, Planübungen, …)

Abschließender Hinweis zum Business Continuity Management

Viele Betreiber von kritischen Infrastrukturen sind in der Regel KMUs und haben oftmals nicht das Budget für umfangreiche BCM-Organisationen und Managementsysteme. Häufig wird dieses Thema maximal von einer Person betreut. Dies ist den Prüfern bewusst und wird auch dementsprechend bewertet.

Business Resilienz

Neben den Anforderungen an das Business Continuity Management eines Unternehmens im Rahmen der Prüfung, zielt das IT-Sicherheitsgesetz grundsätzlich auf die Erhöhung der allgemeinen Business Resilienz der kritischen Infrastrukturen in Deutschland ab.

In der ISO 22301 „Business Continuity Management“ wird der Begriff Resilienz mehrfach verwendet. Nach der eigenen Definition in der ISO Norm behandelt ein BCM den Umgang mit abrupten Störungen, Notfällen und Krisen. Gemäß der ISO 22317 „Security and resilience“ beinhaltet die Resilienz darüber hinaus auch die Fähigkeit sich an Veränderungen des Umfeldes anzupassen. Durch diese Anpassung ist eine gewisse Widerstandsfähigkeit gegenüber kleinen alltäglichen Störungen über akute Schocks bis hin zu inkrementellen Veränderungen gegeben.

Resiliente Unternehmen können somit Chancen und Bedrohungen aus plötzlichen sowie graduellen internen und externen Veränderungen besser erkennen und darauf reagieren. Business Resilienz ist dabei keine eigenständige Management-Disziplin, sondern entsteht aus der Integration etablierter Disziplinen.

Zu diesen etablierten Disziplinen gehören zum Beispiel BCM, ISMS und IT-Security, welche in einem integrierten Managementsystem gesteuert werden können. Da im Rahmen einer KRITIS-Prüfung neben dem BCM gerade auch Anforderungen an das ISMS und die IT-Security gestellt werden hat man automatisch den ersten Schritt in Richtung einer umfassenden Business Resilienz getan.

Somit sollte die hier dargestellte Möglichkeit ein ressourcenschonendes BCM auszubauen als Einstiegpunkt verstanden werden, um zusammen mit der Umsetzung der anderen KRITIS-Anforderungen das eigene Unternehmen resilienter zu machen.

Wie kann ich mich einbringen

Im Sinne der kontinuierlichen Verbesserung setzen wir auf Ihren Beitrag bezüglich Erfahrungen und den vorgeschlagenen Beschreibungen und Hilfsmitteln. Nach der ersten Veröffentlichung sowie Anpassungen bitten wir bis zu einem definierten Zieldatum um Ihre Kommentare. Dies soll zweimal im Jahr möglich sein. Alle Vereinsmitglieder sowie interessierte Kreise werden aktiv informiert, wenn Kommentare wieder möglich sind. Unabhängig davon können Sie uns jederzeit über folgende Adresse kontaktieren: Feedback_Leitfaden@ibcrm.de

Was passiert mit meinem Feedback?

Wir freuen uns über jeden Kommentar, denn unser Ziel ist ein lebendiges Hilfsmittel zu ermöglichen. Wenn Sie uns direkt kontaktieren, werden Sie von uns schnellstmöglich eine Antwort erhalten. Wenn Sie zu Textabschnitten oder Hilfsmitteln während der Kommentierungszeit Anmerkungen abgeben, werden diese nach Sichtung und Bewertung veröffentlicht. Der Kommentator erhält außerdem Rückmeldung, wie mit seinem Verbesserungs- oder Weiterentwicklungsvorschlag umgegangen wurde.

Autorenteam:

Stefanie Fekonja
Marcel Lehmann
Marius Wiersch