Leitlinie

Business Continuity Leitlinie

Version 3.0

01.06.2019

www.aeb.com

Inhalt

1	Geltungsbereich	2
2	Wie wir uns zum Business Continuity Management organisiert haben	2
3	Was wir zum Business Continuity Management organisiert haben	2
4	Grundlegende Leitsätze zum BCM	3
5	Anwendungsbezogene Bereiche	4

Unternehmen, die zur Steuerung und Überwachung ihrer logistischen und außenwirtschaftlichen Prozesse auf AEB-Lösungen setzen, können sich auf Qualität, Betriebs- und Datensicherheit sowie die Ausfallresistenz der angebotenen IT-Services verlassen.

AEB Mitarbeiter bemühen sich nicht nur, um den reibungslosen Ablauf unserer Services zu sichern, sondern machen sich auch proaktiv Gedanken über den Ernstfall: Wo können Störungen auftreten, und wie kann ein optimales Schutzkonzept aussehen? Welche Vorkehrungen müssen getroffen und welche Maßnahmen ergriffen werden, um im unwahrscheinlichen Fall eines Teil- oder gar Komplettausfalls der Systeme möglichst umgehend die Betriebsbereitschaft wiederherstellen zu können?

Die vorliegende AEB Business Continuity Leitlinie beschreibt auf oberster Ebene die Vorgaben und den Rahmen für die Umsetzung für durchgängigen Betrieb.

Im internen Umfeld unterstützen weitere Dokumente wie das **Notfallvorsorgekonzept** und das **Notfallhandbuch** die Umsetzung für ein wirksames Business Continuity Management.

Der **Emergency Guide** regelt Abläufe und Verantwortlichkeiten auch für Notfälle und Desaster Recovery transparent. So können Sie sich auch im Worst Case darauf verlassen, dass der Überblick gewahrt bleibt und die AEB-Services schnell und professionell wieder verfügbar sind.

Zur Sicherstellung der Business Continuity und Wahrung eines hohen Service Levels betreiben wir technische und organisatorische Maßnahmen (gemäß Art. 32 DS-GVO), die wir in unserem **Sicherheitskonzept** zum Ausdruck bringen.

Anmerkungen:

Die AEB hat diese Leitlinie in Anlehnung an den Standard-Baustein (100-4) zum Notfallmanagement des BSI (**Bundesamt für Sicherheit in der Informationstechnik**) und den **ISO-Normen** ISO 22301 und ISO 22313 entwickelt.

Manche internen Details zu Aufbau- und Ablauforganisation, zu betrieblichen Prozessen oder technischen Gegebenheiten können aus Sicherheitsgründen nicht veröffentlicht werden. Dieses Dokument umfasst einen eher strukturellen Überblick über die entsprechenden Bereiche der AEB.

1 Geltungsbereich

Als relevanten Bereich unseres Notfallmanagements - oder, nennen wir es im Folgenden besser **Business Continuity Management (BCM)** - sehen wir unsere gesamte Institution. Wesentlicher Fokus ist die Aufrechterhaltung der angebotenen Cloud-Services für unsere Kunden.

2 Wie wir uns zum Business Continuity Management organisiert haben

Wichtig erscheint uns eine hohe Integration der beteiligten Mitarbeiter in die Prozesse aus IT, Infrastruktur und Services inklusive Rechenzentrum-Betrieb. Daher ist dem Gedanken des BCM keine separate Organisation entsprungen. Die Beschäftigung mit BCM ist für uns als Teil des Risikomanagements ein **selbstverständliches Pflichtfach der Unternehmensführung**. Daher sehen wir Business Continuity Management (BCM) auch in enger Verzahnung mit unserem Informationssicherheitsmanagemensystem (ISMS), zertifiziert nach **ISO 27001**. BCM ist darin als eigener Regelungsbereich definiert.

Folgende wesentlichen Rollen betreiben unser Business Continuity Management:

- Notfall-Beauftragter
- IT-Security Manager
- Einheiten aus IT, Infrastruktur und Operations
- Leitung Services mit Support

Für den Fall der Krise, kann die bereits seit Jahren bei der AEB eingeführte und bewährte Organisation für den **Emergency-Prozess** genutzt werden. Organisatorische Aspekte zu Krisenstab, Kompetenzen und Krisenkommunikation sind dort bereits geregelt.

3 Was wir zum Business Continuity Management organisiert haben

Getreu den Anforderungen des BSI besteht unser Notfallkonzept aus den folgenden zwei Teilen:

Ein Notfallvorsorgekonzept

Darin sind Instrumente enthalten, die uns in die Lage versetzen, unsere Prozesse entsprechend ihrer Relevanz korrekt einzustufen und zu bewerten, um geordnete Notfallmaßnahmen betreiben zu können.

Das Notfallvorsorgekonzept widmet sich dabei sowohl der Prävention (zur Verringerung der Eintrittswahrscheinlichkeit oder auch Verringerung möglicher Schäden) als auch der Notfall-Reaktion.

Das Notfallvorsorgekonzept sieht dazu auch regelmäßige Übungen vor.

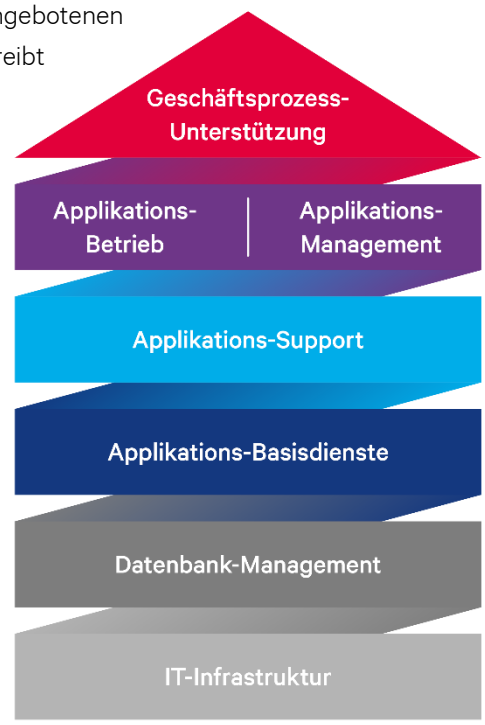
Ein Notfallhandbuch

Darin sind die konkreten Handlungsanweisungen je Service enthalten, um Notfälle geordnet zu bewältigen.

4 Grundlegende Leitsätze zum BCM

1. Im Notfall gilt zunächst die Rettung von Leib und Leben.
2. Die Wiederinbetriebnahme der Geschäftsprozesse unserer Kunden ist danach unser höchstes Anliegen.
3. Der Wiederanlauf ist unverzüglich und entsprechend festgelegter Prioritäten und Regeln vorzunehmen. Dabei haben die Anwendungen für unsere Kunden Vorrang.
4. Sofern nicht direkt in den Regelbetrieb übergegangen werden kann, ist zumindest ein Notbetrieb einzurichten.
5. Zur wirksamen Prävention und stetiger Verbesserung sind regelmäßige Notfallübungen durchzuführen. Deren Befunde fließen qualitätssichernd wieder in das Notfallmanagement ein. Dies gilt auch für die Erkenntnisse aus echten Notfällen.
6. Wichtige Gebote sind Wachsamkeit, Robustheit und einem Denken in „Was wäre, wenn…?“

AEB hat alle innerbetrieblichen Strukturen unter Berücksichtigung der angebotenen Services in einem Modell visualisiert. Das AEB-Applikationsmodell beschreibt sämtliche zu erbringende Leistungen, die für Nutzung, Betrieb und Weiterentwicklung einer Anwendung sichergestellt werden müssen. Bei den Überlegungen und Maßnahmen zur Business Continuity Leitlinie werden die Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik berücksichtigt und auf die Bedürfnisse der AEB und deren Kunden entsprechend übertragen. AEB gleicht die eingesetzten Methoden zur Risikoanalyse und Fehlererkennung mit den Empfehlungen ab und unterzieht damit das eigene Handeln einer laufenden Überprüfung. Ständige Anpassungen, Ergänzungen und Weiterentwicklungen der Prozesse vervollständigen das umfassende Sicherheitskonzept der AEB.



Jedes Segment des AEB-Applikationsmodells unterliegt verschiedenen Sicherheitsvorgaben, die nach sorgfältigen Analysen und entsprechenden Vorstudien als Dienstleistungen von AEB selbst oder von Vertragspartnern erbracht werden.

Die folgende Aufzählung beschreibt die eingesetzten Maßnahmen im Überblick. In jedem Bereich stehen den Mitarbeitern noch detailliertere Anweisungen, Dokumentationen und Hilfsmittel zur Verfügung.

5 Anwendungsbezogene Bereiche

Im Falle der Krise beziehen wir unsere Kunden mit ein, ihnen zu helfen, die Beeinträchtigung aufgrund der Störung möglichst glimpflich zu halten. Ihren Geschäftsprozess im Blick ist die Wiederherstellung des Betriebs dringlicher als die Ursachenforschung. Etwa auch durch Anbieten von Workarounds in möglichst enger Abstimmung. Bereits das Vorsehen solcher Workarounds sehen wir als eine unserer Aufgaben.

Intern sowie auch gemeinsam mit unseren Kunden diskutieren und erarbeiten wir in Workshops Lösungen, basierend auf Was-wäre-wenn-Gedankenspielen als Maßnahme zur weiteren Prävention.

Durch das automatisierte Systemmanagement und die Auswertung der Systemstatistiken und Protokolldateien können Schwachstellen lokalisiert werden, bevor es zu Ausfällen kommt.

Unter Applikationsmanagement verstehen wir nicht nur automatisierte Systemüberwachung, sondern unsere Applikationsmanager haben auch selbst in regelmäßigem Turnus einen Blick auf unsere Applikationen.

Fehler, welche unseren Kunden im System auftreten, werden gezielt disponiert und können bei Bedarf über einen Fernwartungszugang geprüft, erkannt und behandelt werden. Durch ein proaktives (24/7) Monitoring und Alerting der IT, der Infrastruktur und der bereitgestellten Services kann der AEB-Support Ausfälle der AEB-Services zeitnah den betroffenen Kunden mitteilen und weitere Maßnahmen einleiten.

Die Supportabteilung steht in ständigem Austausch untereinander, aber auch in direktem Kontakt mit den AEB IT-Spezialisten der einzelnen Bereiche. Dadurch werden AEB-Kunden auch im Falle einer Störung stets optimal betreut und aktiv und transparent informiert.

Applikations-Basisdienste

Alle kritischen Systemkomponenten sind redundant ausgelegt: Durch Virtualisierungstechniken und Applikationscluster kann die Verfügbarkeit der Systeme schnellstmöglich wiederhergestellt werden. AEB setzt Soft- und Hardware auf bewährtem Stand der Technik ein.

Alle wichtigen Daten werden mehrfach auf einem Storage Area Network (SAN, medienübergreifende Speicherung) gehalten. Für Reaktions- und Ausfallzeiten oder Prioritäten bestimmter Services können auf Wunsch und nach Bedarf des Kunden verschiedene Modelle angeboten werden.

Nachträgliche Erweiterungen der Services oder der verfügbaren Rechenleistung können auf Nachfrage jederzeit dynamisch vorgenommen werden. Engpässe können dadurch unkompliziert erkannt oder vermieden werden.

Datenbank-Management

Für die AEB Datenbankservices stehen eigens ausgebildete Datenbankadministratoren im Haus zur Verfügung. Darüber hinaus bestehen Dienstleistungsverträge mit externen Datenbankspezialisten, die sich je nach Wunsch und Bedarf des Kunden rund um die Uhr um die Betreuung und – wenn doch mal erforderlich – die Wiederherstellung der Systeme und Daten bemühen. Eine mehrstufige Sicherung der Daten erfolgt mehrmals täglich. Eine Sicherungskopie wird regelmäßig in einen anderen Brandabschnitt ausgelagert.

IT-Infrastruktur

Die IT-Infrastruktur-Schicht wird aus eigener Hand und unter Zuhilfenahme weiterer externer, sorgfältig ausgewählter Sicherheits-Dienstleister für die folgenden damit verbundenen Dienstleistungen bereitgestellt:

- grundlegende Stromversorgung und USV
- Brandschutz
- Klimaanlage und
- Zutrittskontrolle.

Das Rechenzentrum wird rund um die Uhr nicht nur von intern, sondern auch von extern über eine Remoteverbindung überwacht. Die redundante Internetanbindung stellt die hohe Verfügbarkeit der AEB Services sicher. Die Anbindung zum Rechenzentrum des Bundesfinanzministeriums zur Abwicklung des elektronischen Zollverfahrens ist über eine Betriebs- und eine Ausfall-Leitung

sichergestellt. Die eingesetzte Hardware entspricht dem bewährten Stand der Technik und wird von unseren Hardwarelieferanten über Kundendienstvereinbarungen gewartet.

Während der regelmäßig stattfindenden Wartungsarbeiten werden Notfallübungen nach den vorhandenen Verfahrensanweisungen und Prozessen durchgeführt, die dabei ständig weiter optimiert werden. So stellen wir sicher, dass möglicherweise auftretende Störungen jederzeit schnell und routiniert behoben werden können.

AEB legt besonders großen Wert auf Aus- und Weiterbildung: AEB Mitarbeiter im IT- und Servicebereich bilden sich laufend weiter und können auf umfassendes Know-how zurückgreifen.

AEB SE . Hauptsitz . Sigmaringer Straße 109 . 70567 Stuttgart . Deutschland . +49 711 72842 0 . www.aeb.com . info.de@aeb.com . Registergericht: Amtsgericht Stuttgart . HRB 767 414 . Geschäftsführende Direktoren: Matthias Kieß, Markus Meißner . Vorsitzende des Verwaltungsrats: Maria Meißner

Standorte

Düsseldorf . Hamburg . Lübeck . Mainz . Malmö . München . New York . Paris . Prag . Rotterdam . Salzburg . Singapur . Soest . Stuttgart . Warwick . Zürich