



Kongresse & Seminare

IT-Sicherheit in der Produktion

Business Continuity





- Unternehmensstandort Hamburg
- gegründet 1.4. 2005
- langjährige Beratungserfahrungen
 - Business Continuity
 - Information Security
 - Service Quality
- bei Großunternehmen und Mittelstand
 - Banken und Versicherungen
 - Industrie und Handel
 - Logistik- und Medienunternehmen
 - Behörden
- Wir helfen unseren Kunden,
 - ihre Geschäftsfähigkeit gegen operationelle Risiken abzusichern
 - und so ihre Wettbewerbsfähigkeit zu verbessern.





Inhalte

- Was versteht man unter Business Continuity (BC) ?
- Bedrohungen für die BC eines Unternehmens
- Umgang mit Bedrohungsszenarien
- Trends und zukünftige Ursachen für Betriebsunterbrechungen



Was versteht man unter Business Continuity?



Business Continuity - Definition

British Standard 25999-1:2006 BCM-Part 1 Code of Practice

Strategische und taktische Fähigkeit einer Organisation in Bezug auf mögliche **Störfälle** und **Geschäftsunterbrechungen**

- **vorsorglich zu planen** und
- auf deren Eintreten zu **reagieren**,

mit dem Ziel den **Geschäftsbetrieb** in einem akzeptablen, **zuvor festgelegten Maße weiterzuführen**



Business Continuity Management - Definition

British Standard 25999-1:2006 BCM-Part 1 Code of Practice

Ganzheitlicher *Management-Prozess*,

- mit dessen Hilfe mögliche *Bedrohungen* für eine Organisation sowie die bei deren Eintritt resultierenden *Auswirkungen* auf den Geschäftsbetrieb *identifiziert* werden,
- der einen *Rahmen* bildet, die Widerstandsfähigkeit der Organisation durch die Fähigkeit zu einer *wirksamen Reaktion* auszubauen,
- so dass die Belange der wichtigsten Interessensgruppen gewährleistet sind
- sowie das Ansehen, der Markenname und die wertschöpfenden Tätigkeiten der Organisation geschützt werden.



BCM versus IT-Sicherheit

- **Business Continuity Management**
 - sichert die angemessene Verfügbarkeit und Wiederherstellung kritischer Ressourcen (über die IT hinaus !), die zur Ausübung kritische Geschäftsfunktionen benötigt werden
- **IT-Sicherheits-Management**
 - sichert angemessene Verfügbarkeit, Vertraulichkeit, Integrität, Verbindlichkeit der IT
 - betrachtet meist auch BC bezogen auf IT
 - ISO 17799, Kap. 14, „Business Continuity Management“
 - Grundschatz, z.B. Maßnahmenkatalog M6 Notfallvorsorge
- **klare Absprache und Abgrenzung notwendig**



Bedrohungen für die BC eines Unternehmens



Typische Bedrohungen

- Systemstörungen und -ausfälle (Anlagen / IT / Netz)
- Personen, die schädliche Handlungen ausführen
 - z.B. Diebstahl, Sabotage, Hacker, Versehen
- Angriffe auf die IT
 - z.B. Viren, DoS
- Ausfall benötigter Zulieferungen, Versorgungsleistungen und Dienstleistungen
 - z.B. Stromausfall, Leitungsstörung
- Personalausfall
 - z.B. durch Krankheit, Streik
- Brand, Explosion
- Umgebungs- und Nachbarschaftsgefahren
 - z.B. durch Lagerung und Verarbeitung von Gefahrgütern
- Elementargefahren
 - z.B. Überschwemmung, Sturm
- Unzureichende Unternehmensprozesse

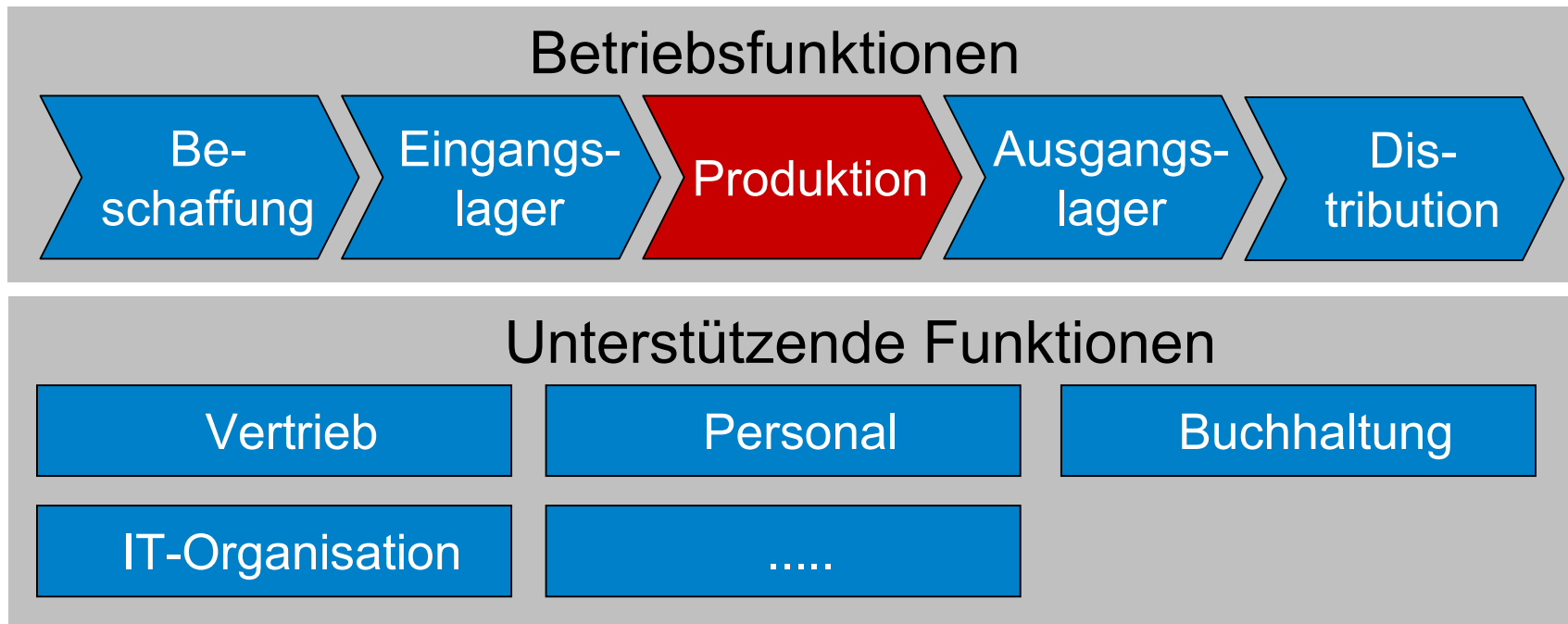


Umgang mit Bedrohungsszenarien



Identifikation kritischer Geschäftsfunktionen

- Untersuchung des möglichen Schadens der durch den Ausfall von Geschäftsfunktionen entsteht
- Die Produktion als wertschöpfender Prozess ist grundsätzlich als kritisch zu betrachten

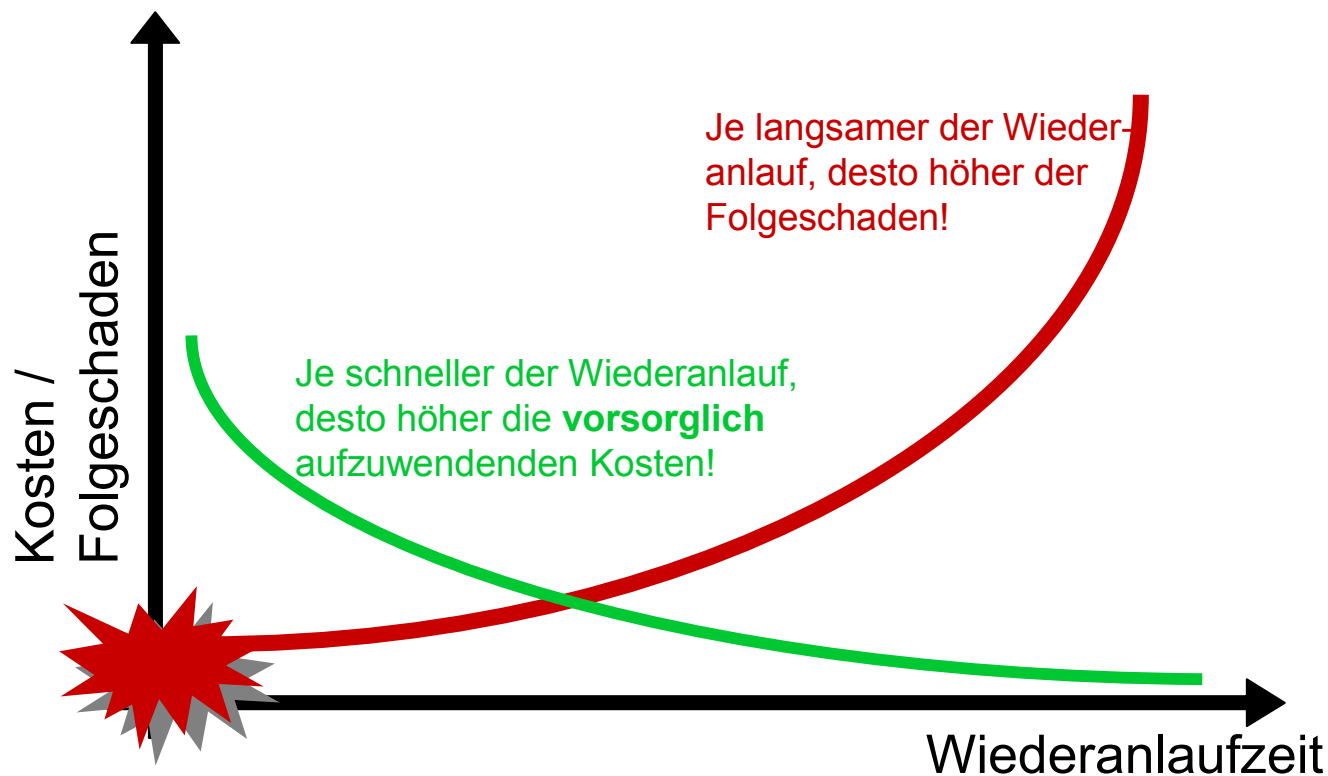




Festlegung der Wiederanlaufziele

Wie lange darf der Ausfall einer Geschäftsfunktion maximal dauern (Wiederanlaufzeit)?

- Workshop mit GF-Vertretern
- Schadensverlauf über der Zeitachse





Spezielle Betrachtung der IT

- IT ist kritische Ressource
- Abbildung der Wiederanlaufziele der Geschäftsfunktionen auf die IT
 - Betrachtung der IT-Anwendungen
 - max. zulässige Wiederanlaufzeit
 - zusätzlich max. zulässiger Datenverlustzeit
 - Wiederanlaufklassen

WAK	Wiederanlaufzeit	Datenverlustzeit	Erläuterung
1	Annähernd 0	Annähernd 0	„Heiße“ Wiederanlauflösung (z.B. Cluster / Datenspiegelung / Datenreplikation)
2	4h	Annähernd 0	„Heiße“ Wiederanlauflösung (z.B. Ersatzrechner / Datenspiegelung / Datenreplikation)
3	1 Tag	1 Tag	„Warme“ Lösung (z.B. vorhandener Test-Server wird zum Produktions-Server umkonfiguriert)
4	3 Tage	1 Tag	„Warme“ Lösung (z.B. Datenvolumen ⇔ Restore-Fähigkeit)
5	7 Tage	1 Tag	„Kalte“ Lösung (z.B. Lieferverträge für HW)
6	> 7 Tage	1 Tag	Keine Vorhaltung einer Notfalllösung

- Wiederanlaufklassen der IT-Anwendungen auf IT-Systeme und Netze abbilden



Betrachtung weiterer kritischer Ressourcen

- Mitarbeiter
- Gebäudeinfrastruktur
- Arbeitsplätze
- Produktionsanlagen
- Unterlagen (Vital Records)
- Versorgungsinfrastruktur (Strom / Wasser /)
- Zulieferungen
-



Betrachtung der Bedrohungen

Handlungsoptionen

1. Eintrittswahrscheinlichkeit verringern (Prävention)
2. Dauer und Auswirkung des Ausfalls verringern (Reaktion)
 - bei unternehmensgefährdender Auswirkung zusätzlich zu 1.
 - wenn Eintrittswahrscheinlichkeit nicht senkbar ist
3. Risiko übertragen (z.B. Versicherung, Auslagerung)
 - wenn kostengünstiger
 - unternehmerische Verantwortung bleibt bei Auslagerung bestehen (Kontrollpflicht)
4. Akzeptieren
 - bei sehr geringer Auswirkung
 - bei extrem geringer Wahrscheinlichkeit
5. Geschäftsfunktion ändern oder einstellen



Realisierung reaktiver Maßnahmen

Vorsorge zur Verringerung der Dauer und Auswirkung umfassender Ausfälle ist oft nicht ausreichend geregelt

- Planbare (Ausfall-)Szenarien festlegen
 - Im Back-Office Bereich, z.B.
 - Ausfall des Hauptverwaltungsgebäudes
 - Ausfall des Rechenzentrums
 - Im Produktionsbereich
 - Unternehmensindividuell (z.B. Ausfall einer Leitstelle)
- Wiederanlaufstrategie erstellen und umsetzen
- Ablauf- und Aufbauorganisation festlegen
 - Alarmierung / Eskalation
 - Ersthilfe / Sofortmaßnahmen
 - Wiederanlauf
- Dokumentieren (BC-Plan)
- Testen / Pflegen



Trends und zukünftige Ursachen für Betriebsunterbrechungen



Trends und Ursachen – Produktions-IT

IT-Trends	Künftige Ursachen für Betriebsunterbrechungen
<ul style="list-style-type: none">• Gewicht und Komplexität der IT steigt auch in Produktion• Einzug von Standard-IT in die Produktionsumgebung• Konvergenz Backoffice- und Industrienetze<ul style="list-style-type: none">• Verbindungen zum Büronetz und zu Fremdfirmen• Nutzung gemeinsamer Infrastruktur• Kriminalisierung und Professionalisierung der Hackerszene	<ul style="list-style-type: none">• Ungewollte Fortpflanzung von Störungen• Gezielte Angriffe auch auf die Produktions-IT

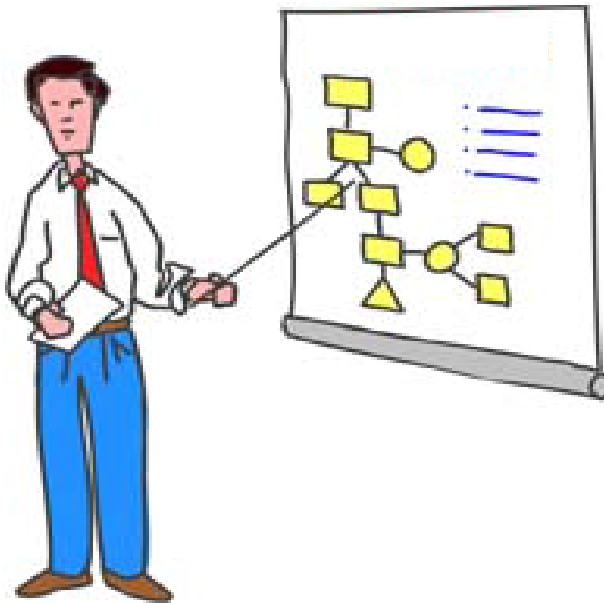


Trends und Ursachen - Sonstige

Trends	Künftige Ursachen für Betriebsunterbrechungen
<ul style="list-style-type: none">• Globaler Austausch	<ul style="list-style-type: none">• Pandemie<ul style="list-style-type: none">• Personalausfälle• Ausfälle von Versorgungs- und Dienstleistungen
<ul style="list-style-type: none">• Qualitätsverschlechterung von Versorgungsleistungen	<ul style="list-style-type: none">• Ausfall von Strom, Wasser, Gas, Netzen
<ul style="list-style-type: none">• Wachsende politische Instabilität / Krieg der Kulturen	<ul style="list-style-type: none">• Unruhen / Terroristische Anschläge / Cyberterrorismus
<ul style="list-style-type: none">• Veränderung der Arbeitswelt	<ul style="list-style-type: none">• Sabotage
<ul style="list-style-type: none">• Beeinflussung der Umwelt	<ul style="list-style-type: none">• Naturkatastrophen<ul style="list-style-type: none">• Sturm• Wasser• Schnee



Vielen Dank für Ihre Aufmerksamkeit!



Dipl.-Ing.

Stefan Gunzelmann

Geschäftsführer

consequa GmbH
Süderstraße 73
20097 Hamburg
www.consequa.de

Tel.: 040 / 78 89 70 63
Fax: 040 / 78 89 70 66

stefan.gunzelmann@consequa.de