EDITH GERMANY
Enabling **Digital Innovation & Technology** in Hesse
Co-funded by the European Union
ATHENE
Fraunhofer SIT

CyberUp im Rahmen der EDITH-Initiative

Notfälle vorbereiten –Notfallpläne und Business Continuity

18. März 2024

Motivation

Ob Cybersicherheitsvorfälle, Naturkatastrophen, unzufriedene Mitarbeiter oder technische Probleme, diese Dinge passieren

JEDEN TAG

Notfallplan oder Business Continuity Management?

Was ist der Unterschied?

Notfallplan ist die „kleine“ Version
- Üblich für einzelne denkbare Vorfälle, z. B. Informationssicherheits-Notfälle (IS-Notfälle); in diesem Vortrag Beispiele dazu
- Notfallpläne sind eine leicht skalierbare Lösung, gerade für KMU

Business Continuity Management (BCM) ist deutlich umfangreicher
- berücksichtigt alle Arten von „Vorfällen“ (Szenarien), die den Betrieb behindern,
- komplettes Managementsystem vorgesehen,
- BCM ist im Rahmen von Zertifizierungen (z. B. TISAX) sinnvoll
- BCM wird häufiger erwähnt:
  - geltende Standards und Gesetze
  - Konkurrenz

Notfallplan - Incident Management

- Aufgabenstellung:
  - Etablierung eines Prozesses zum angemessenen Umgang mit Sicherheitsvorfällen

- Ziele:
  - Reaktionsfähigkeit
    (rasches Erkennen und Melden)
  - Einschätzungsfähigkeit
    (lokal lösbares Problem oder gravierender Vorfall)
  - Handlungsfähigkeit
  - Schadensminimierung
  - Beweissicherung und Identifikation der Täter
  - Effektivität und Effizienz

- Ggf. Einordnung in das ISM des Unternehmens
  Strategische Ausrichtung: Verantwortung Unternehmensleitung

Auslöser für IT-Sicherheitsvorfälle und „Incident Response“-Prozess

- Benutzerfehlverhalten, das zu Datenverlust oder sicherheitskritischer Änderung von Systemparametern führt
- Sicherheitslücken in Hardware- oder Softwarekomponenten
- massenhaftes Auftreten von Computer-Viren
- Gehackter Webserver
- Offenlegung vertraulicher Daten
- Kriminelle Handlungen wie Einbruch oder Diebstahl
- …

Gebraucht wird:

- Planung und Vorbereitung
- Entdeckung und Berichten (Strukturierte Aufbereitung)
- Bewertung und Entscheidung
- Schadenbegrenzung, -behebung und Wiederherstellung, forensische Analyse
- „Post Incident“-Aktivitäten (Lessons Learned) zur zukünftigen Vorbeugung von Vorfällen

Teilprozess – Vorbereitung

- Definition Incident Response Policy
  - Einleitung
  - Zweck der Policy
  - IR-Verfahren und -Prozesse
  - Verantwortlichkeiten
  - Dokumentation
- Definition von Incident-Kategorien
- Entwicklung eines Priorisierungsschemas

- Einrichtung einer IR-Struktur
  - Entwicklung und Dokumentation eines Incident Management, das die Policy unterstützt
  - Kommunikationswege und -vorrichtungen
  - Information Security Incident Response Team (**->** CERT)
  - Testschemata
- Werkzeuge & Ressourcen

- Auswahl von Incident Kategorien:
  - Denial of Service
  - Information Gathering
  - Zugriffsverletzung
  - Malware
  - …

- Faktoren für die Priorisierung
  - Funktionale Auswirkungen
  - Auswirkungen auf Datenbestände
  - Wiederherstellungsaufwand

- Werkzeuge & Ressourcen:
  - Formulare
  - Kommunikationspläne und -wege
  - Forensik
  - Netzwerk Diagramme
  - …

Teilprozess – Entdeckung und Analyse


Quelle: http://pixelquelle.de

- Entdeckung
  - Automatisch, z. B. durch IT-Monitoring der IT-Infrastrukturen
    - Intrusion Detection System – IDS
    - Security Information and Event Management (SIEM)
    - Anti-Viren-Software
    - Regelbasierte Logfile-Analyse
  - Automatisch durch Monitoring der Infrastruktur
    - Gefahrenmeldeanlagen
  - Manuell durch interne Mitarbeiter oder Externe
- Verantwortliche alarmieren
- Einordnung in die Incident-Kategorie
- Dokumentation des Incidents
  - Zeitpunkt und Ort des Ereignisses – Alle Rechner und Server sollten die gleiche Systemzeit haben
  - Mögliche Ursachen oder Auslöser
  - Die aktuellen Auswirkungen
  - …
- Analyse des Incidents (Einstufung)
- Priorisierung des Incidents
  - Schadensausmaß (aktuell bzw. potentiell), kein, gering, mittel, hoch
  - Wiederherstellungsaufwand, normal, erweitert, risikoreich, Eskalation

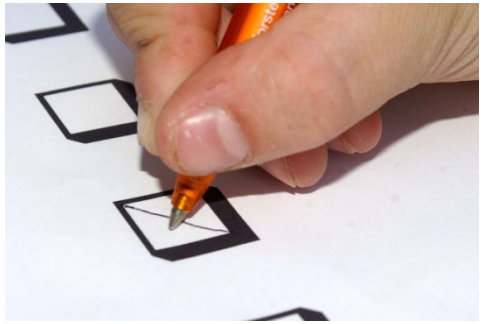
Teilprozess – Reaktion
Schadensbegrenzung, -behebung und Wiederherstellung

- Vorgehen ist abhängig vom jeweiligen Incident:
  - Schaden für Geschäftsprozess / System / Ressource / Applikation?
  - Folgen des Abschaltens oder Isolieren?
  - Beweissicherung notwendig?
  - Zeit und zur Verfügung stehende Ressourcen?
  - Potenzial für das Entstehen weiterer Schäden?
  - Müssen Vorgaben für die Verfügbarkeit von Services eingehalten werden?
  - …

Quelle: http://pixelquelle.de

Teilprozess – Post Incident

- „Lesson learned“
  - Verbesserung und Optimierung
    - Was passierte genau, warum und zu welcher Zeit?
    - Wie schnell und effektiv erfolgte die Reaktion?
    - Welche Informationen/Ressourcen fehlten?
    - Würde das Team nochmals so handeln?
    - Welche Maßnahmen, Prozesse, Tools sind zu verbessern oder neu aufzunehmen?
    - …
- Gegenschläge (Hackbacks) in Deutschland rechtlich unzulässig



Quelle: http://pixelquelle.de

Kernaussagen zum Incident Management

- Incident Management bezieht sich auf das Erkennen und die Handhabung von IT-Sicherheitsvorfällen
- Die Reaktion auf einen Vorfall ist abhängig von
  - den verfügbaren Ressourcen
  - dem zu erwartenden Schadensumfang
  - den eingerichteten Prozessen
- Die Verantwortung für die strategische Ausrichtung liegt bei der Unternehmensleitung
- Eine Dokumentation ist zwingend notwendig
- Zentrale Anlaufstelle für präventive und reaktive Maßnahmen bieten sogenannte **CERTs** (Computer Emergency Response Team)

CERT - Hauptaufgaben

- Aktive Suche nach neuen Gefahren und deren Analyse
- Bearbeitung von Anfragen zu Sicherheitsvorfällen
- Analyse eingehender Vorfallmeldungen
- Forensische Analysen, (z. B. „artifact handling“)
- Erstellen und Veröffentlichen von präventiven Handlungsempfehlungen
- Hinweise zu Schwachstellen in Hard- und Softwareprodukten
- Warnen und informieren bei besonderen Bedrohungslagen
- Empfehlungen für reaktive Maßnahmen zur Schadensbegrenzung
- … Zusammenarbeit mit anderen CERTS, auch international

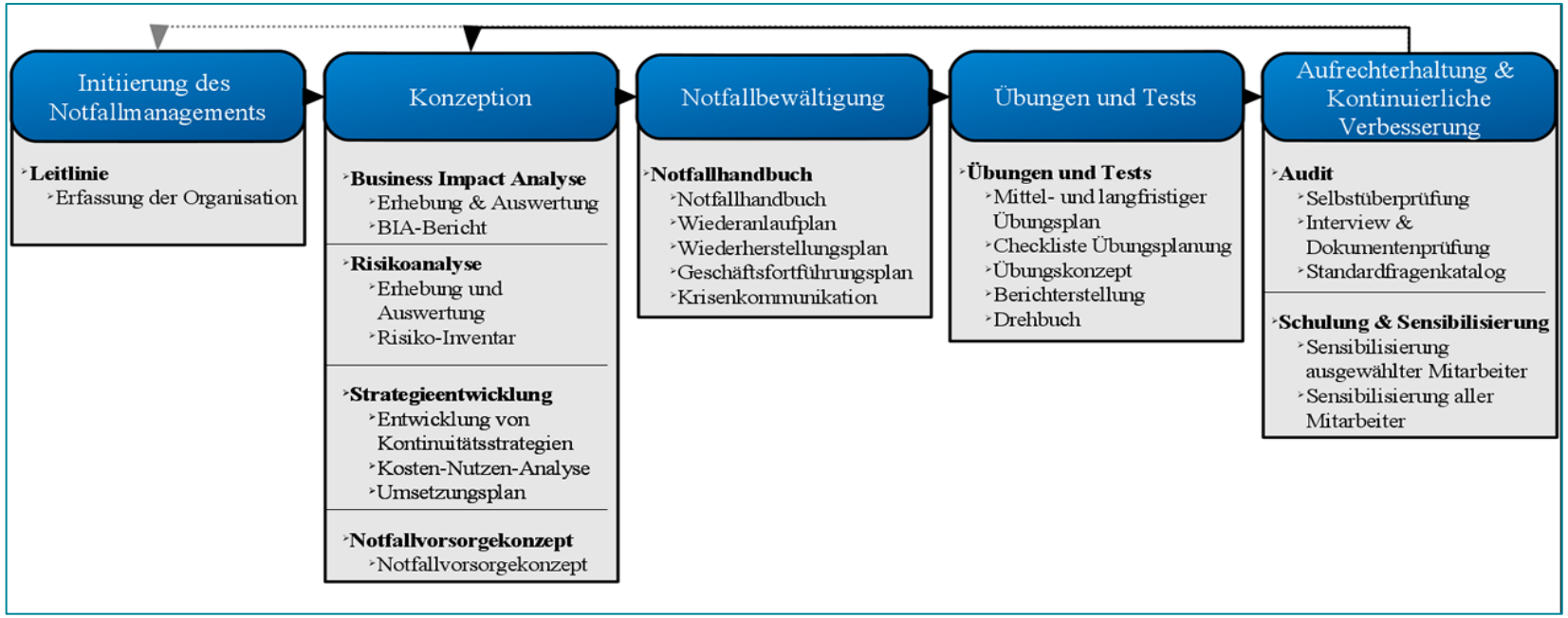
Kernaussagen zu CERTs:

- CERTS bieten proaktive und reaktive Dienstleistungen im Zusammenhang mit Sicherheitsvorfällen
- Abhängig von der Zielsetzung können die charakterliche Ausprägung, die Organisationsstruktur und der Fokus der Leistungen variieren
- Nationale und internationale Kooperationen ermöglichen Synergieeffekte und die schnellere Entdeckung von neuen Angriffsformen

Umsetzungsrahmenwerk zum Notfallmanagement nach BSI-Standard 100-4

Hilfestellung des BSI zur Implementierung eines Notfallmanagementsystems mit Leitfäden, Textvorlagen, Muster für Workshop-Präsentationen für alle Phasen des Systems

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-100-4-Notfallmanagement/Umsetzungsrahmenwerk-zum-Notfallmanagement-nach-BSI-Standard-100-4/umsetzungsrahmenwerk-zum-notfallmanagement-nach-bsi-standard-100-4_node.html



Weitere Informationen zu IT-Notfallplänen (IS-Incident Management)

- **ISO/IEC 27035:2016 Part 1 und 2**
  Information technology – Security techniques –
  Information security incident management
  Principles of IM, Guidelines to plan an prepare for IR
- **NIST Special Publication 800-61:2012**
  Computer Security Incident Handling Guide. Recommendations http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
- **Mining gold... A primer on incident handling and response**
  Autor: Stacy Jordan. SANS Institute InfoSec Reading Room.
  http://www.sans.org/reading_room/whitepapers/incident/mining_gold__a_primer_on_incident_handling_and_response_32818
- **BSI-Leitfaden "IT-Forensik", 2011**
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/Leitfaden_IT-Forensik_pdf.pdf?__blob=publicationFile

Business Continuity Management (BCM) - Was bedeutet das?

- Aufrechterhaltung, Fortsetzung oder Wiederherstellung der Betriebsfähigkeit bei einem Störfall, egal welcher Art (auf einem akzeptablen, zuvor festgelegten Produktivitätsniveau)
- BCM ist der Prozess zur Aufrechterhaltung der Betriebsfähigkeit kritischer Geschäftsprozesse
- BCM dient der Vorbereitung,
  - um mit Vorfällen mit Betriebsunterbrechung umzugehen und
  - um weiterhin die Geschäftsziele zu erreichen
  - um die wirtschaftliche Existenz nicht zu gefährden

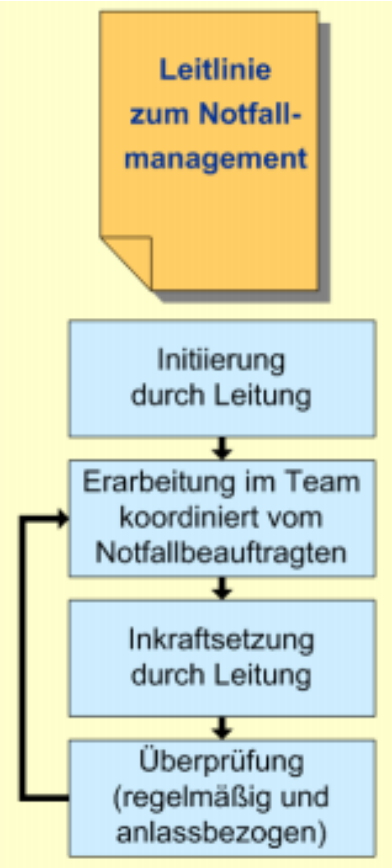
Ziele:

- Sicherung der Stabilität (zeit-) kritischer Geschäftsprozesse
- Begrenzung des Gesamtschadens, z. B.
  - bei umfangreichem Personalausfall wg. Krankheit
  - bei umfänglichen Dateninkonsistenzen oder Datenverlust
  - …
- Beschreibung, wie der Betrieb in einer stark veränderten Umgebung und mit weniger Ressourcen weitergeführt werden kann
- Wiederherstellung aller Funktionen, um zu einem Produktivitätsniveau wie vor dem Ereignis zu gelangen

BCM initiieren und BCM-Leitlinie („Policy“)

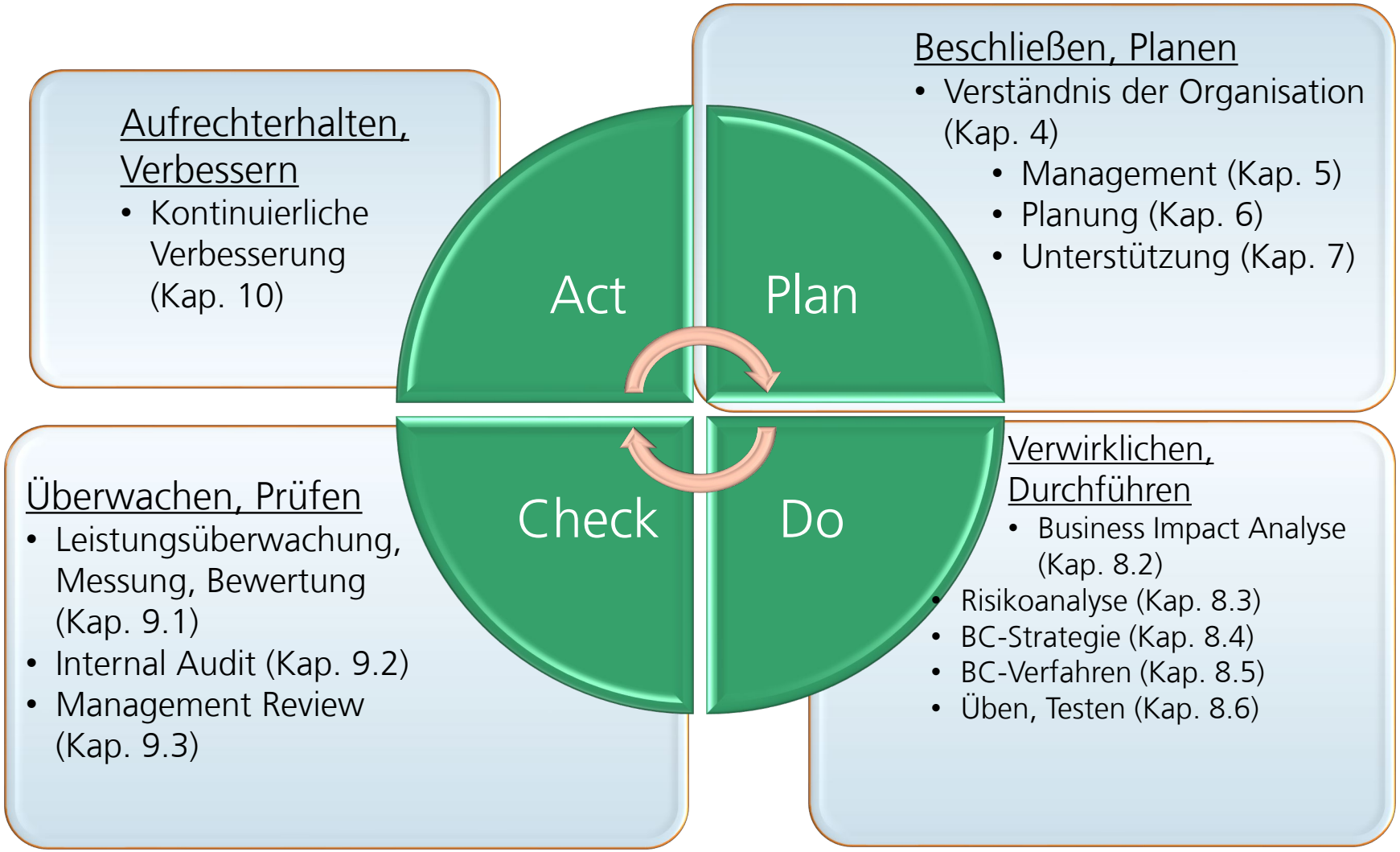
- Das Management überzeugen
  - BCM muss „verkauft“ werden

- Notfallbeauftragter
- Von Projektteam erarbeitetes Grundsatzdokument
- abgestimmt mit IT-Sicherheitskonzept, Revision, Risikomanagement, u. a.
- Von Unternehmensleitung unterschrieben (Absichtserklärung)
- Inhalt:
  - Grundsätzliche Zielsetzungen (warum ein BCMS?)
  - Wesentliche Rahmenbedingungen
  - Verfolgte Prinzipien (Methoden und Prozessschritte)
- Verbindlicher Auftrag an Mitarbeiter zur Mitwirkung



Quelle: BSI-Standard 100-4, Webkurs

BCM-Prozess als PDCA Zyklus nach ISO 22301

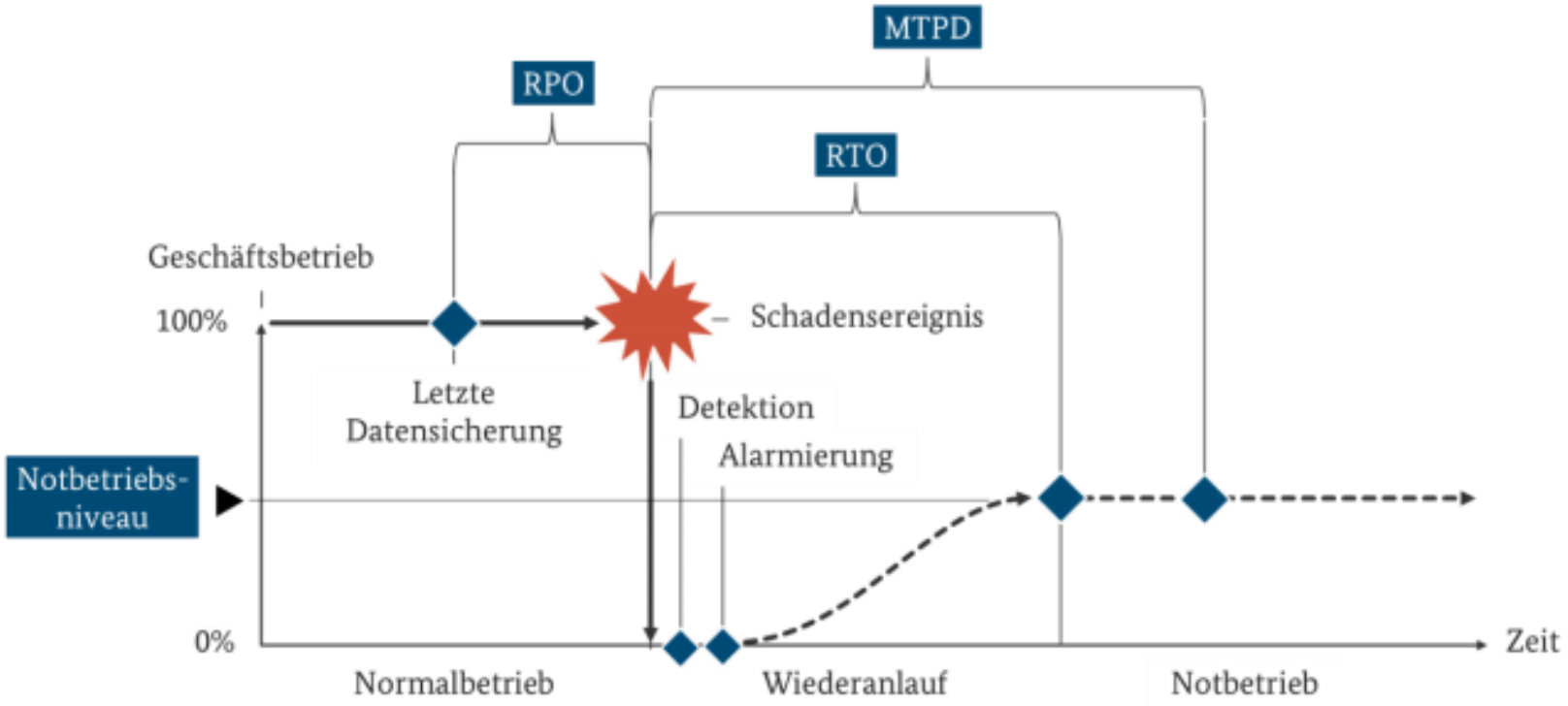


Ziel: Notfallkonzept

- Das Notfallkonzept besteht aus zwei Komponenten:
  - Notfallvorsorgekonzept (präventiv)
  - Notfallhandbuch (reaktiv)
- Planungsschritte
  - Business Impact Analyse
  - Risikoanalyse
  - Entwicklung von Optionen für die Kontinuitätsstrategie mit Alternativen von Notfall- und Notfallvorsorgemaßnahmen
- Maßnahmen
  - Zur Verbesserung der Reaktion auf Störungen (Prozessunterbrechungen)
  - Zur effizienten Wiederherstellung der Geschäftstätigkeit
  - Zur Reduktion der Auswirkungen von Störfällen

Do – Kenngrößen, Verfügbarkeitsziele und Zeitverlauf

- Maximal tolerierbare Ausfallzeit, MTA
  (MTPD, Max. tolerable Period of Disruption)
- Wiederanlaufzeit, WAZ (RTO, Recovery Time Objective)
  → Grundlage für BCM-Strategie
- Wiederanlauf-Niveau
- Maximal tolerierbare Notbetriebszeit (-niveau), MTN
- Maximal tolerierbare Wiederherstellungszeit, MTW
- Maximal tolerierbarer Datenverlust, (RPO, Recovery Point Objective)
  → Grundlage für Backup-Strategie



Quelle: BSI-Standard 200-4, Draft

Do - „Business Impact“-Analyse (BIA)

- Unternehmensziele und -werte verstehen lernen
- Untersuchung und Bewertung der quantitativen und qualitativen Auswirkungen einer Unterbrechung von Geschäftsprozessen
  z. B. durch **Nutzung von Störfallszenarien**
- Inventarisierung der Geschäftsprozesse mit
  - Auswirkungen eines Ausfalls: finanziell, juristisch, Image …
  - Ausweichmöglichkeiten
  - Abhängigkeiten (Input, Output)
  - Benötigten Ressourcen (Technik, Infrastruktur, Mitarbeiter …) für Normal- und Notbetrieb
- Grundlage ist eine abzustimmende Klassifikation, zum Beispiel „unkritisch“, „kritisch“, „sehr kritisch“
- Zeitliche Dimension betrachten: Ab wann wird der Ausfall eines Prozesses kritisch?

Schadensszenarien:

- Finanzielle Auswirkungen
- Beeinträchtigung der Aufgabenerfüllung
- Verstoß gegen Gesetze, Vorschriften und Verträge
- Negative Innen- und Außenwirkung (Imageschaden)
- Beeinträchtigung der persönlichen Unversehrtheit

Vorgehen:

Fragebogen

▼

Interviews

▼

Analyse

▼

Ggf. vertiefende Interviews

▼

BIA-Bericht

Abgrenzung von Schadenskategorien - Beispiel

Schadenskategorie „normal“	
finanzielle Auswirkungen	Der finanzielle Schaden bleibt für die Institution tolerabel (z. B. Verlust weniger als 5-20% des Umsatzes)
Beeinträchtigung der Aufgabenerfüllung	Beeinträchtigung wird von Mitarbeitern toleriert / andere Tätigkeiten können vorgezogen werden / Nacharbeit behindert die Aufgabenerfüllung nicht merklich / andere Organisationseinheiten oder Vertragspartner werden in ihrer Arbeit nicht wesentlich gestört
Verstoß gegen Gesetze, etc.	Verstöße gegen Gesetze und Bestimmungen mit geringen Konsequenzen / Verstöße werden nur intern bemerkt
negative Innen- und Außenwirkung	Störungen bzw. Ausfälle werden nur in Einzelfällen bemerkt und von Kunden und Geschäftspartnern als bedeutungslos eingeschätzt / Kunden und Geschäftspartner ziehen keine Konsequenzen / das grundsätzliche Vertrauen in die Institution ist nicht beeinträchtigt / keine wahrnehmbaren Verluste von Marktanteilen

Do – BCM-Risikoanalyse

- Analyse und Bewertung der Wahrscheinlichkeit eines Ausfalls kritischer Ressourcen (aus BIA) und der damit verbundenen Auswirkungen auf die Geschäftsprozesse
- Erstellung einer Gefährdungsübersicht
  (gemäß BSI 200-3 auf Basis der elementaren Gefährdungen)
- Verfahren z. B. nach BSI 200-3
- Ergebnis:
  Grundlage für gezielte Notfallvorsorgemaßnahmen und BC-Lösungen unter Kosten-Nutzen-Risiko-Gesichtspunkten

Vorgehen:

Fragebogen mit Risikofaktoren

▼

Interviews

▼

Analyse

▼

Ggf. vertiefende Interviews

▼

Recherchen zur Risikosituation

▼

RIA-Bericht

Do - „Develop your plan“

- Entwicklung von BC-Strategien
  - Zur Auswahl alternativer Betriebsmethoden zur Aufrechterhaltung kritischer Prozesse gemäß Priorität und Zeitplan
  - Vermeidung von Single Points of Failures in unternehmenskritischen Prozessen
  - Zur Festlegung der Wiederherstellungsziele
- Ebenen der BC-Strategie
  - Organisation
  - Prozesse
  - Ressourcen

BC-Ressourcen für Normal- und Notbetrieb

- Personal
- Informationen
- Informationstechnologie
- Infrastruktur (Gebäude, Arbeitsplätze, Stromversorgung…)
- Dienstleistungen/Dienstleister
- Spezialgeräte

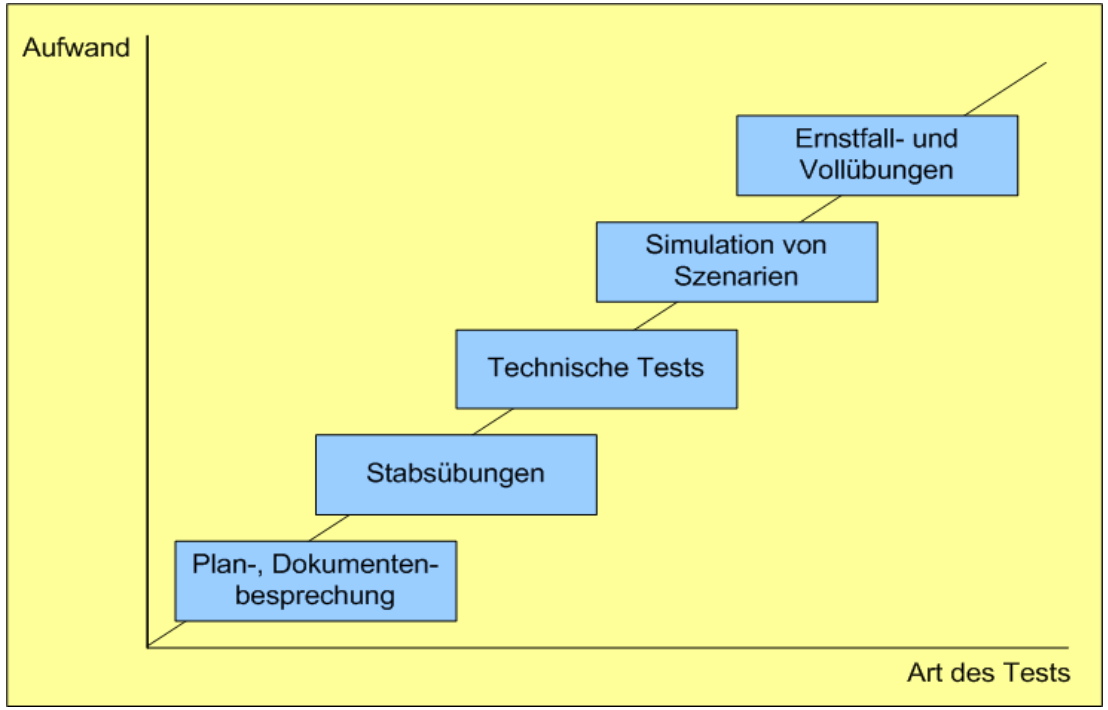
→ Erhebung und Bewertung der Kritikalität der Ressourcen

BC - Strategien

Optionen	Kurzbeschreibung	Risikopotential
Minimallösung	Nur besonders exponierte Prozesse absichern; Teilprävention; Kostenbegrenzung hat Priorität	Hohes Restrisiko, hohes Schadenspotential
Kleine Lösung	Präventionsmöglichkeiten zu begrenzten Kosten nutzen, Prozesse der Priorität 1 möglichst vollständig, Priorität 2 teilweise absichern	Mittleres Restrisiko, begrenztes direktes Schadenspotential
Mittlere Lösung	Umfassende Absicherung aller Prozesse mit Priorität 1, weitgehende Maßnahmen für Prozesse der Priorität 2, Teilabsicherung der niedrig priorisierten Prozesse	Mittleres Restrisiko, geringes direktes Schadenspotential
Große Lösung	Umfassende Robustheitsstrategie, Redesign oder Redundanz für Prozesse der Prioritäten 1 und 2, Verstärktes Outsourcing von Prozessen niedriger Priorität	Geringes Restrisiko, Minimierung des Schadenspotentials

Check und Act – Leistungsüberprüfung und Bericht

- Ziel:
  - Überprüfung der Angemessenheit, Wirksamkeit und Effizienz
  - Erkennung von Korrekturbedarf und Verbesserungsmöglichkeiten
- Voraussetzung:
  - Test- und Auditkonzept
  - „Drehbücher“ mit verschiedenen Notfall-Szenarien



Dokumente und Anforderungen

- Anforderungen an die Dokumentation:
  - aktuell
  - verfügbar
  - verständlich und praktikabel
  - vertraulich

- BCM - Leitlinie
- Rollenbeschreibungen mit
  - Aufgaben
  - Rechten
  - Pflichten

- Übersicht über notw. Ressourcen
- Notfallvorsorgekonzept
- Notfallhandbuch
- Protokolle z. B von Tests und Audits
- Informationsfluss und Meldewege
- …

BCM in Standards und Gesetzen

- Notfallmanagement wird explizit oder implizit zunehmend zum Bestandteil von gesetzlichen Vorschriften, Anforderungen zur Corporate Governance und Sicherheitsmanagement-Standards.
- Beispiele:
  - Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin): Mindestanforderungen an Risikomanagement (MA Risk) und Kreditgeschäft (MaK)
  - Basel III (IV)
  - KonTraG
  - ISO 27000 ff
  - CobiT
  - Aktiengesetz
  - …

BCM: Normen und Standards (Auswahl)

- National Institute of Standards and Technology
  NIST 800-34: Contingency Planning Guide for Federal Information Systems (2010) (csrc.nist.gov)
- ISO 22301:2020
  Security and resilience – Business continuity management systems – Requirements
- ISO 22313:2020
  Societal security – Business continuity management systems – Guidance
- ISO 27031:2011
  ICT-Readiness for business continuity
- BSI-Standard 200-4 BCM (https://www.bsi.bund.de); praxisnahe Anleitung, um ein Business Continuity Management-System (BCMS) in der eigenen Institution aufzubauen und zu etablieren; Im Gegensatz zum BSI-Standard 100-4 und UMRA sind im BSI-Standard 200-4 die einzelnen Prozessschritte bereits detailliert beschrieben. Somit entfallen die ergänzenden Modulbeschreibungen aus dem Umsetzungsrahmenwerk

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

Vorbereitungskurs zur Zertifizierung

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

7 Themenbereiche der IT-Sicherheit:

- Sicherheitsmanagement
- IT-Sicherheit und Recht
- Systemsicherheit
- Grundlagen Netzwerksicherheit
- Kryptografie
- Cloud Security
- Virtualisierung

Mehr Informationen und Termine: https://www.sit.fraunhofer.de/de/tisp/

Vielen Dank für Ihre Aufmerksamkeit

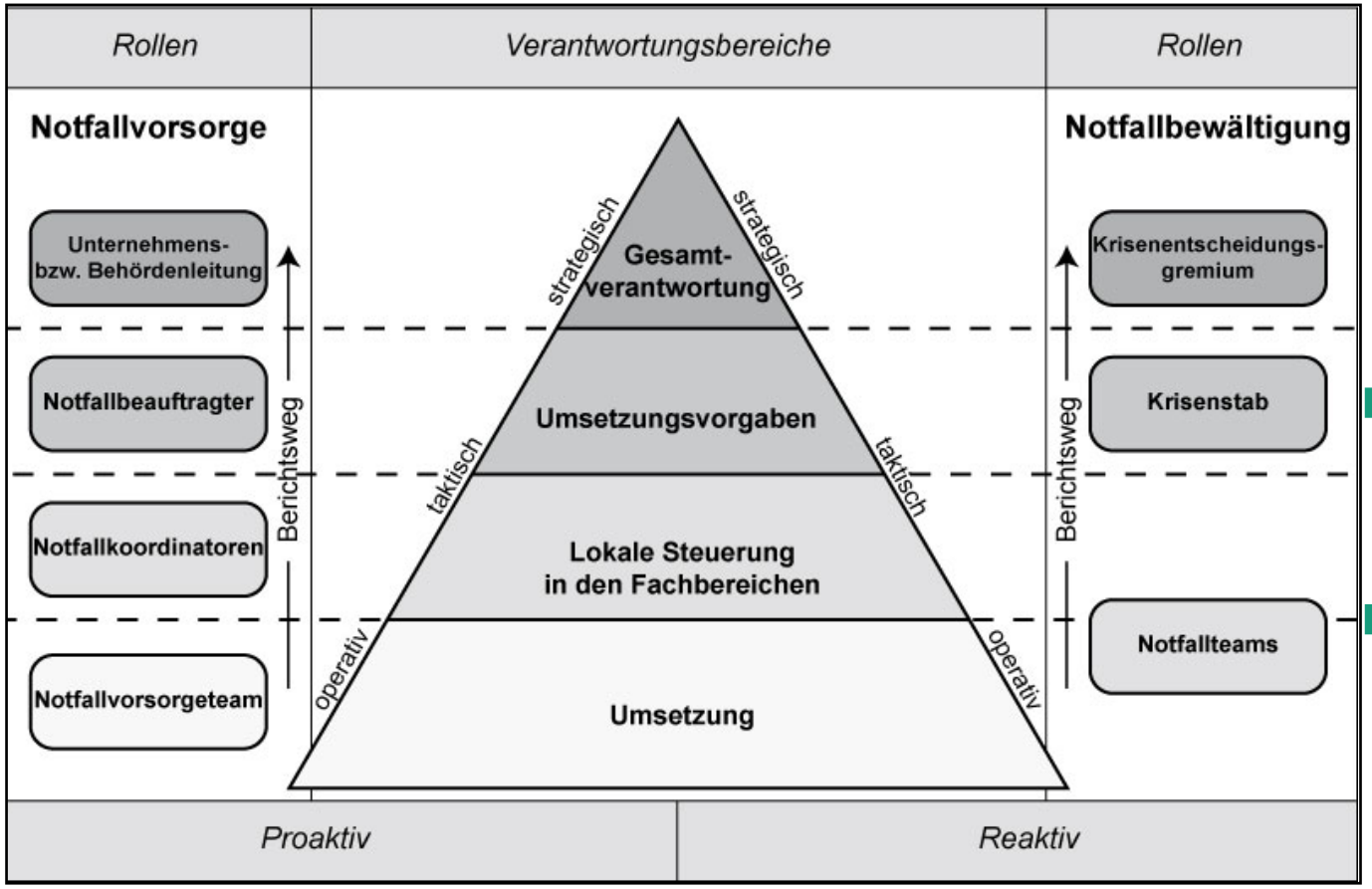
Fraunhofer SIT

Kontakt

Dr. Henrik Rüterjans
Tel. +49 6151 869-289
vorname.name@fraunhofer.de

Fraunhofer SIT
Rheinstraße 75
64295 Darmstadt
www.sit.fraunhofer.de

Beispiel: BCM-Rollen und Verantwortungsbereiche



Erfasst und bewertet
die Lage,
koordiniert Notfallteams

Ersatzbeschaffung,
Analyse der Störungsursache