Master of (IT-)Disaster - Willkommen im Chaos!

Jan Frongia & Nina Lausen

Nina Lausen
Senior Consultant

- Beratung zu den Themen ISMS, BCM und ITSCM
- Umsetzung von Anforderungen aus BSI 200-4, ISO 22301 und ISO 27001
- Definition, Implementierung und Weiterentwicklung von vollumfänglichen ISM-, BCM- und ITSCM-Systemen

Qualifikationen

- Master of Science - Wirtschaftsinformatik
- ISO 27001 ISMS & ISO 22301 BCMS Lead Auditor
- BSI IT-Grundschutz Praktiker
- Zusätzliche Prüfverfahrens-Kompetenz für § 8a BSIG
- ITIL 4 - Foundation Certificate IT Service Management

Jan Frongia
Managing Consultant

- Experte für IT-Infrastruktur
- Langjährige Erfahrung in Aufbau, Betrieb und Wiederherstellung von komplexen Infrastrukturen
- Mitglied im Prüfungsgremium der IHK Niederbayern/Oberpfalz
  - Ausbildung und Verbreitung von IT-Wissen im Beruf Fachinformatiker für Systemintegration
- Verantwortlicher des Themenfeldes ITSCM
  - Krisenvorbereitung von Betrieben und Institutionen mit technisch ausgereiftem Notfallmanagement
- Technische Unterstützung bei Incident-Response-Einsätzen

Agenda

1. Willkommen im Chaos!
2. Gewinner in der Krise sein!

Willkommen im Chaos!

Exkurs: Cyber Incident Response Erfahrungsbericht

Infizierung

- Direkter oder indirekter Angriff
- Versendung von Informationen
- Ggf. weitere manuelle Kompromittierung
- Erweiterung der Rechte
- Extraktion von Daten

Mo	Di	Mi	Do	Fr	Sa	So
28	29	30	31	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Infizierung Angriff

Januar Februar März

- Reduzierung von Sicherheitsmechanismen
- Löschen von Backups, Schattenkopien
- Roll-out Kryptotrojaner
- Erpressung

Mo	Di	Mi	Do	Fr	Sa	So
28	29	30	31	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

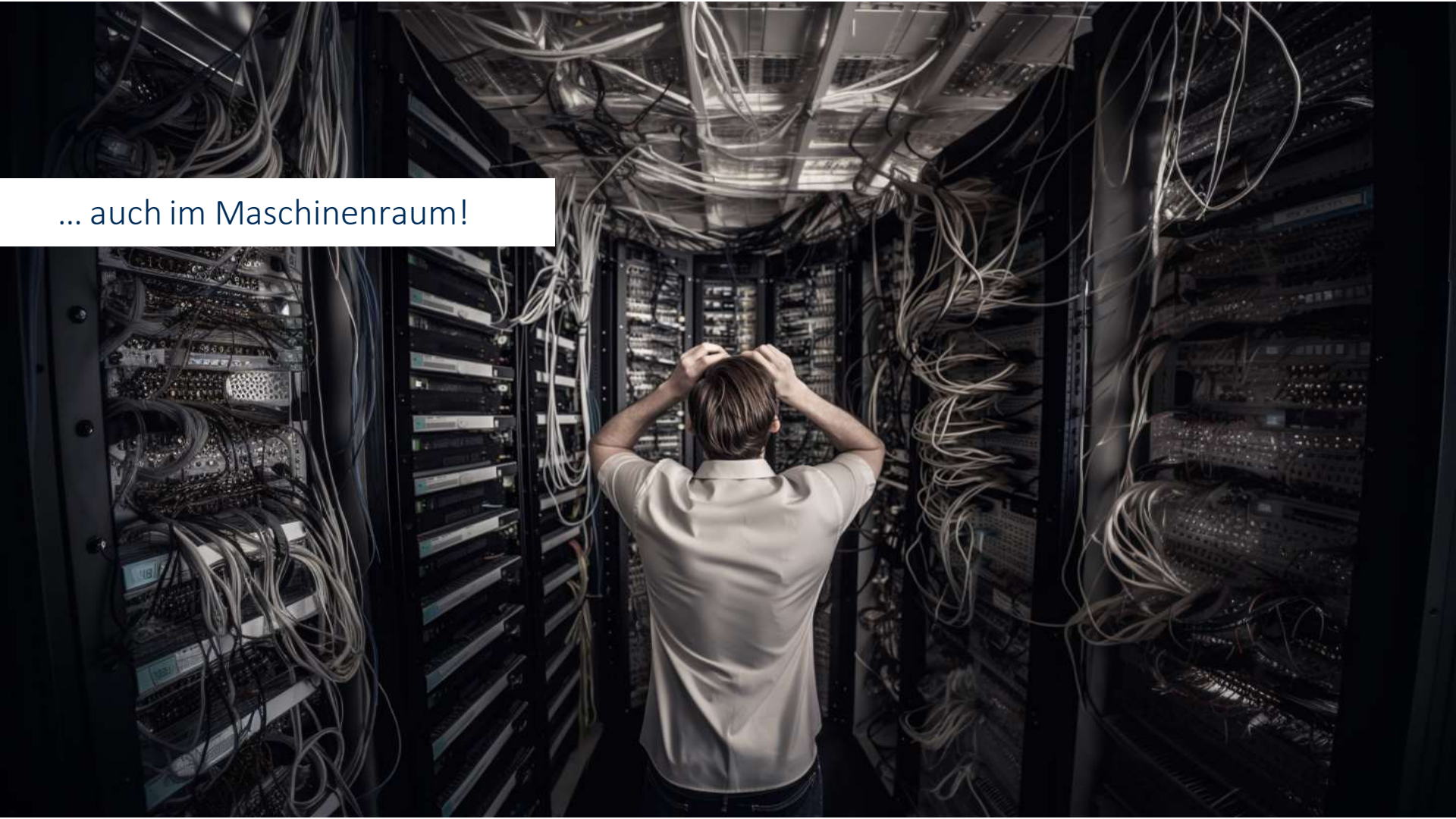
Infizierung Angriff Chaos

Januar Februar März

- Detektion häufig Usergetrieben
- Paralysiert, fassungslos, gelähmt
- Impulsgetriebene Erstreaktion
- Alle konzentrieren sich auf die IT

… es herrscht Chaos …

Mo	Di	Mi	Do	Fr	Sa	So
28	29	30	31	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31


… auch im Maschinenraum!

Infizierung Angriff Chaos

Januar Februar März

- Wiederaufbau der IT-Landschaft (Wunsch)
- Häufig fehlt Know-how
- Backups nur bedingt/nicht nutzbar
- Notbetriebsprozesse werden verzögert aufgebaut
- Mangelnde interne sowie externe Kommunikation
- Maßnahmentracking fällt schwer
- Belegschaft hoch motiviert - Ressource Mensch wird jedoch außer Acht gelassen

Mo	Di	Mi	Do	Fr	Sa	So
28	29	30	31	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

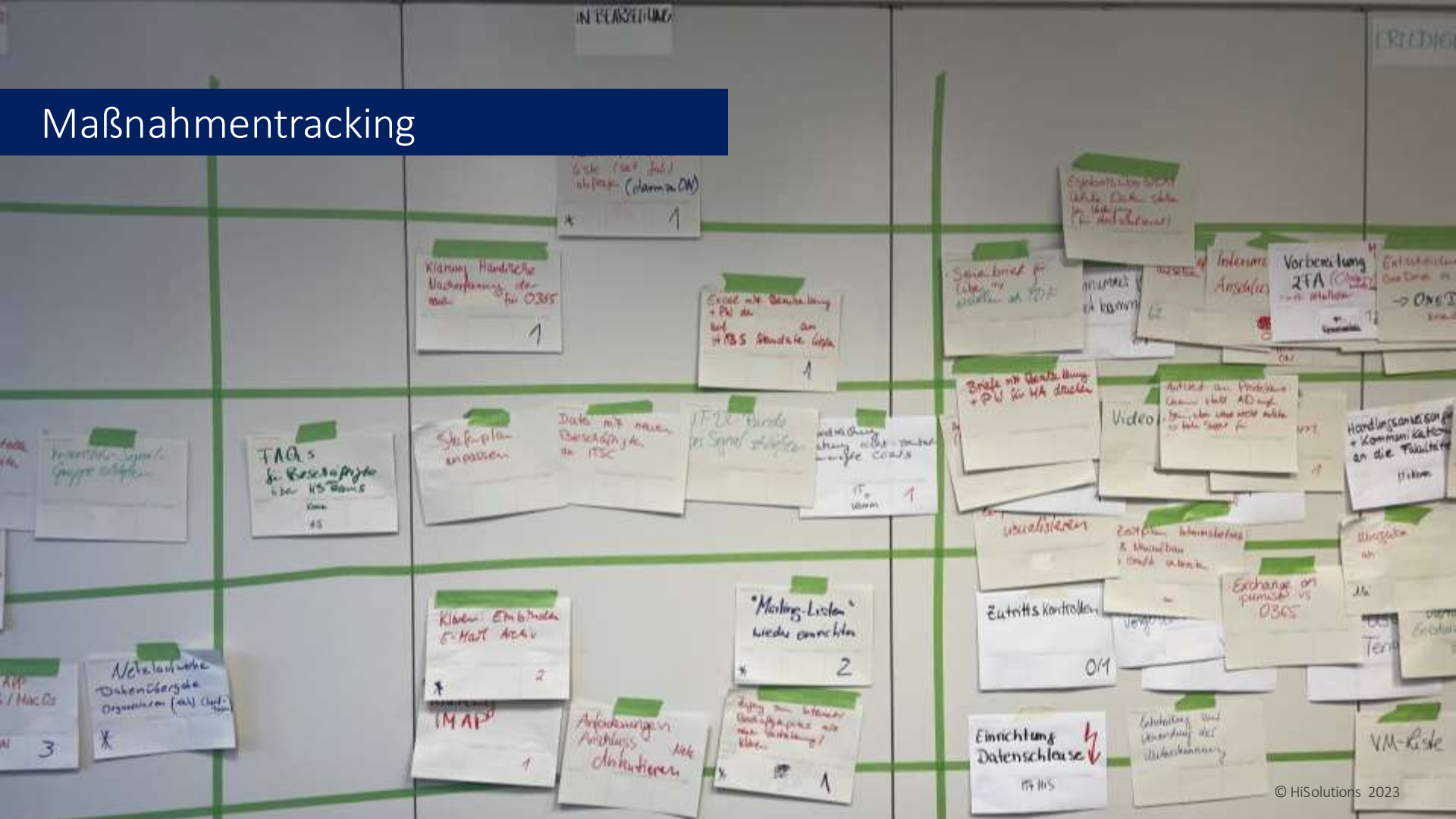
Infizierung Angriff Chaos **Konstituierung**

Januar Februar März

- Es entsteht eine Art „Regelbetrieb“
- Notbetriebsprozesse greifen zunehmend
- Weiterentwicklung fällt schwer
- Ermüdungserscheinungen nehmen zu
- Motivation und zielgerichteter Einsatz der Mitarbeiter

Mo	Di	Mi	Do	Fr	Sa	So
28	29	30	31	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Maßnahmentracking



Infizierung Angriff Chaos Konstituierung **Stabiler Notbetrieb**

Januar Februar März

- Paralleler Aufbau der IT-Landschaft
- Viele weitere Prozesse werden zeitkritisch
- Feinarbeiten und Details werden sichtbar
- Steuerung und Kommunikation der neuen Aufgaben

Nächster Monat

Mo	Di	Mi	Do	Fr	Sa	So
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28

- Kleinarbeiten dauern i. d. R. mehrere Monate
- Daten aus den Notprozessen werden sukzessive zurückgeführt
- Hohe Lernkurve/Awareness über die eigene (IT-)Sicherheit

→ Siehe Phase Störbetrieb (BSI-Standard 200-4)

Mo	Di	Mi	Do	Fr	Sa	So
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28

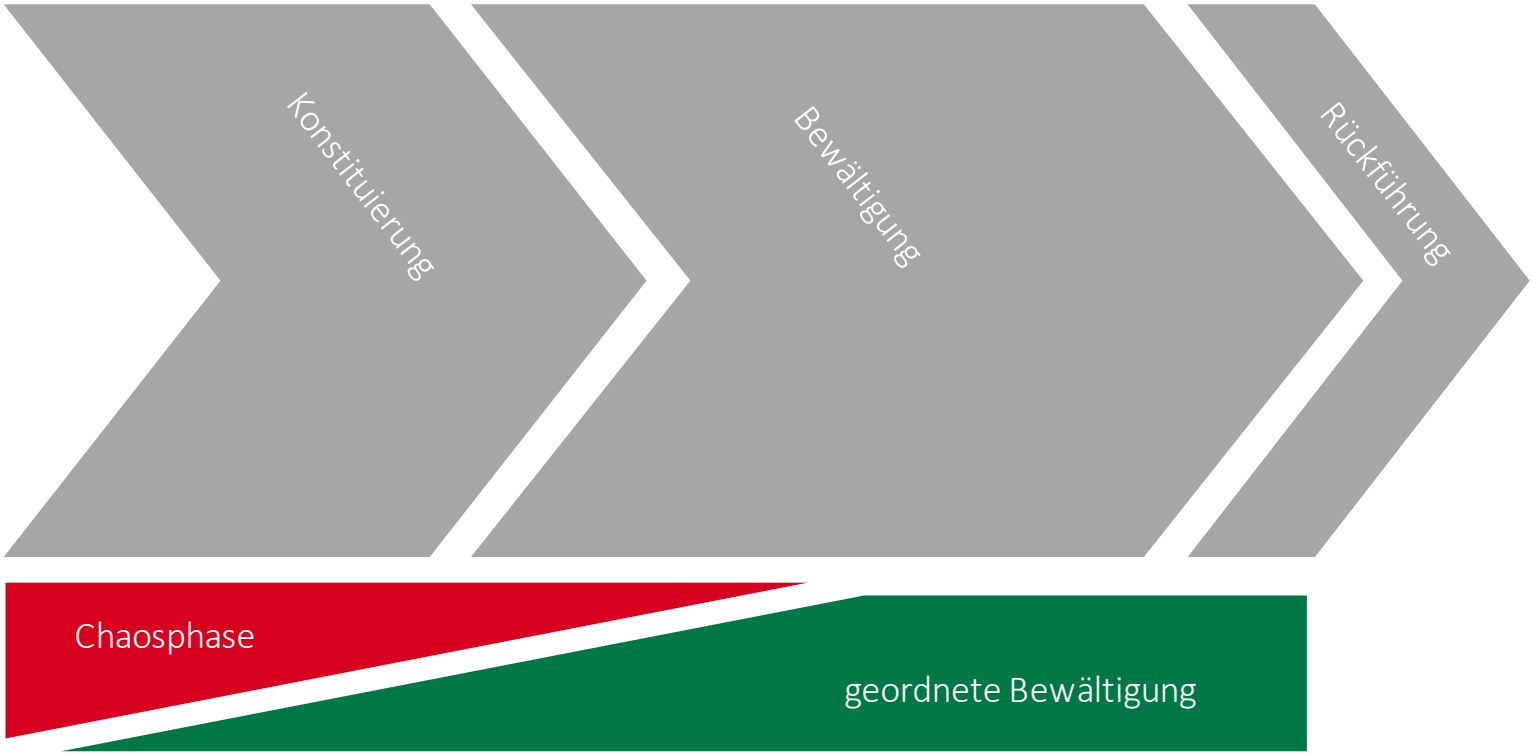
Weiterer Monat

Mo	Di	Mi	Do	Fr	Sa	So
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28

Gewinner in der Krise sein!

Krise ist ein produktiver Zustand.
Man muss ihm nur den Beigeschmack der Katastrophe nehmen.
- Max Frisch, 1978

Ziel ist die Chaosphase so kurz wie möglich zu halten



Wie lässt sich ITSCM von BCM abgrenzen?

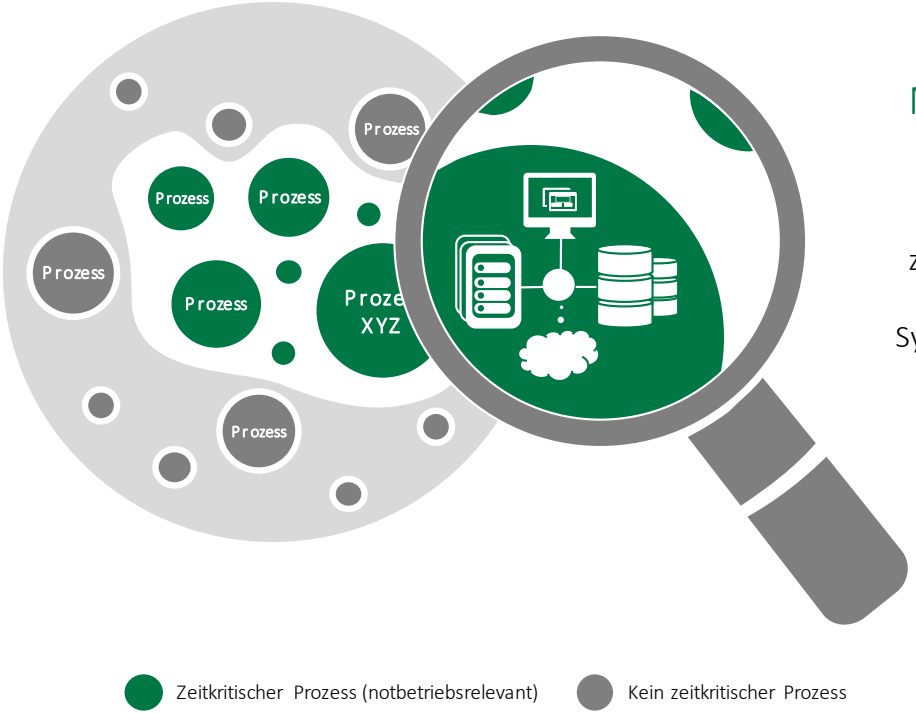
Abgrenzung BCM und ITSCM

Business Continuity Management (BCM)

dient dem Schutz der zeitkritischen Geschäftsprozesse gegen ungeplante Unterbrechungen infolge des Eintritts eines Ereignisses mit hohem Schadenspotential

Beteiligte:

Gesamtorganisation



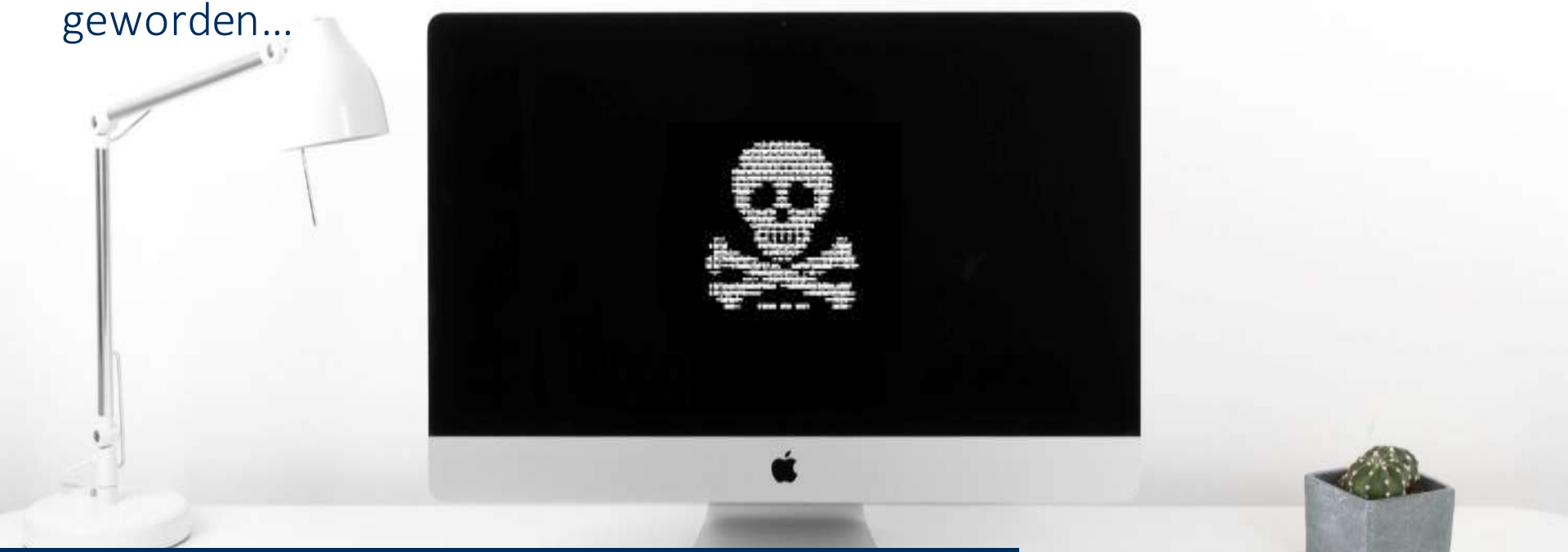
IT Service Continuity Management (ITSCM)

dient der Aufrechterhaltung und raschen Wiederherstellung von zeitkritischen IT-Services und deren zugrundliegende IT-Systemen und IT-Ressourcen in einem IT-Notfall

Beteiligte:

IT

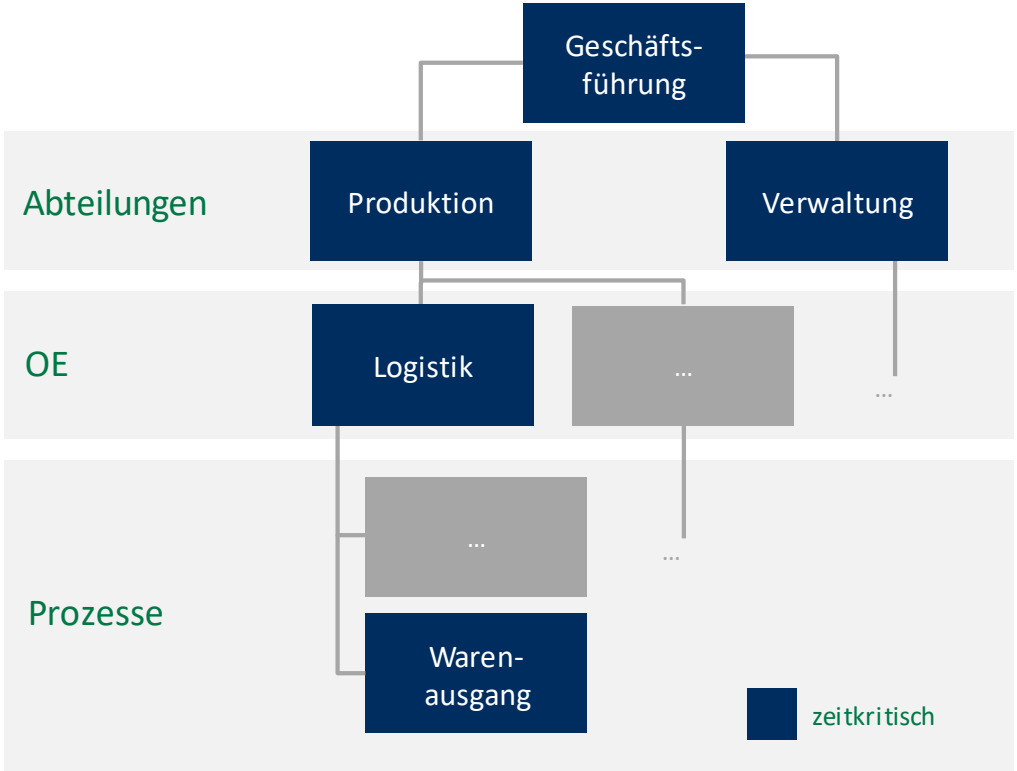
Stellen Sie sich vor, Ihr Unternehmen ist Opfer eines Cyberangriffs geworden…



Ihre gesamte Organisation steht still und es herrscht Chaos…

… und Sie fragen sich: „Was muss eigentlich als Erstes wieder laufen?“

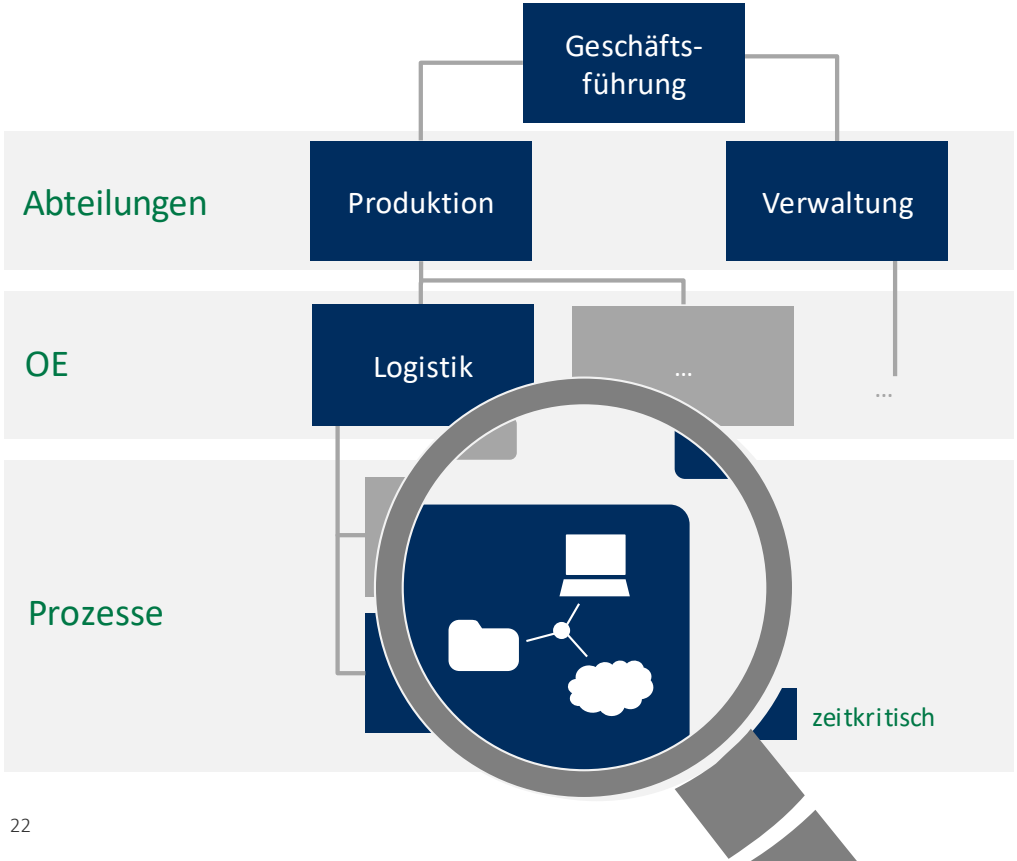
Kronjuwelen kennen



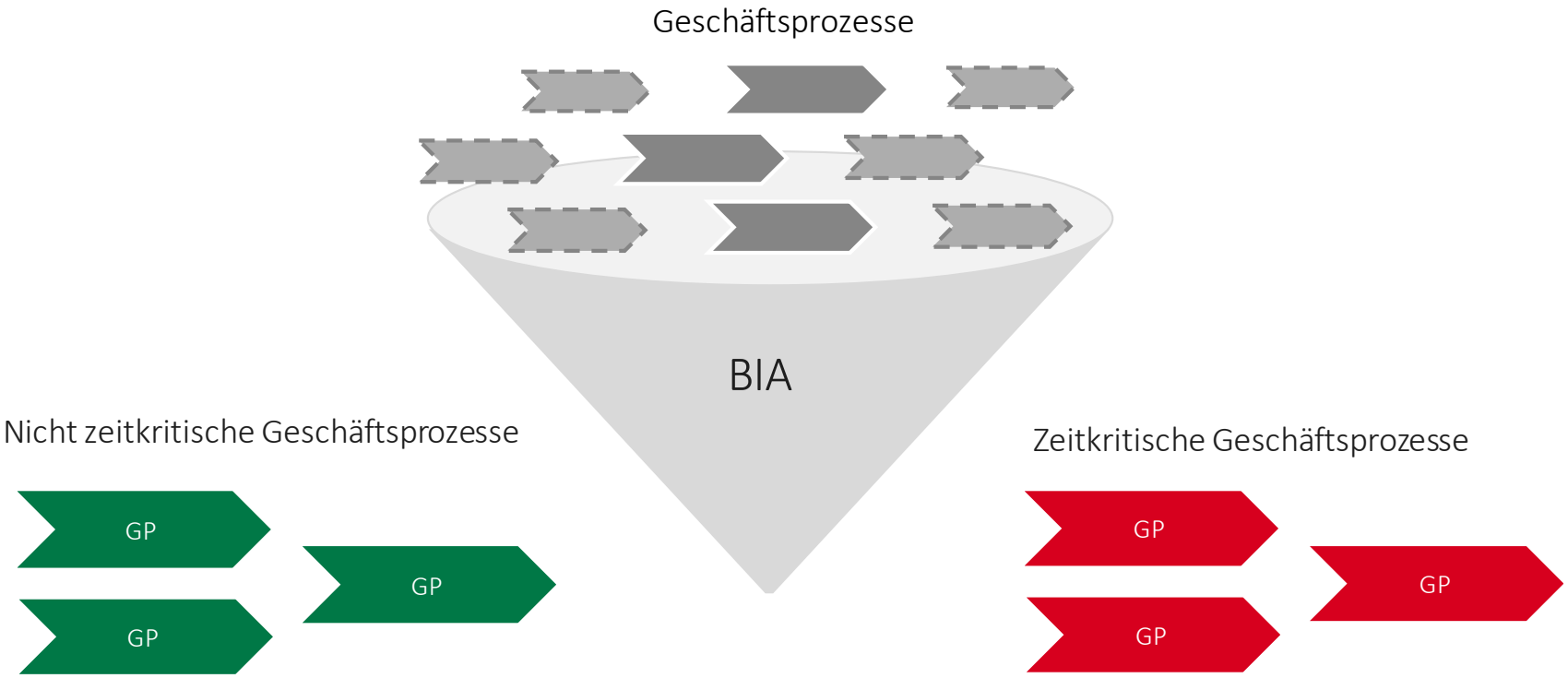
Leid(t)frage:
Welche Organisationseinheiten schmerzen bei einem Ausfall von *einer Woche* richtig?

Sinnvoll, aber zeitaufwändig wäre eine weiterführende Priorisierung im Rahmen einer **Business Impact Analyse** (BIA).

IT-Abhängigkeiten identifizieren und priorisieren



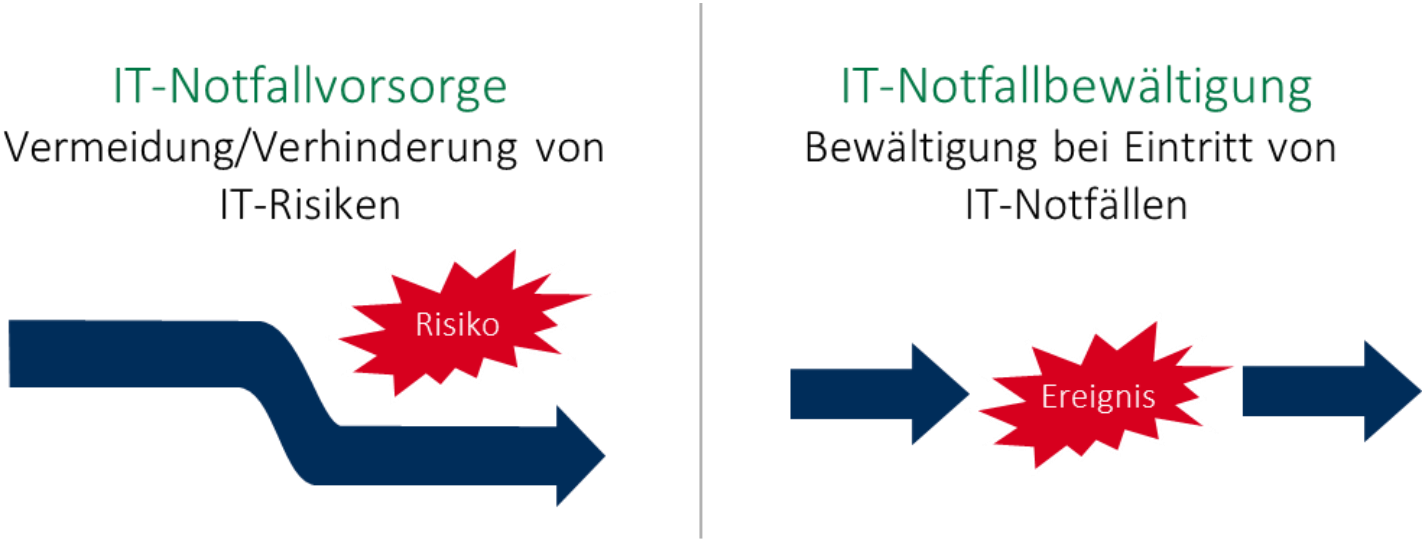
Die BIA hat das Ziel die zeitkritischen Prozesse eines Unternehmens zu identifizieren



Die BIA liefert folgende Ergebnisse

- Die BIA hinsichtlich des ITSCM umfasst hierzu die:
  - Identifikation der zeitkritischen Geschäftsprozesse sowie der zeitkritischen IT-Services und deren notfallrelevante Abhängigkeiten (maximal tolerierbare Ausfallzeit; MTA)
  - Wiederanlaufzeiten der zeitkritischen IT-Services (Recovery Time Objective; RTO)
  - Maximal zulässiger Datenverlust (Recovery Point Objective; RPO)
  - Ermittlung der notfallrelevanten Ressourcen (z. B. Anzahl Notfallarbeitsplätze)
- Anhand einer Strukturanalyse können die komplexen Abhängigkeiten der IT-Assets ermittelt werden (siehe IT-Grundschutz Vorgehensweise).

ITSCM gliedert sich in 2 Phasen



Erfahrungswert: In vielen (IT-)Notfallhandbüchern sind für die Reaktion unnötige Informationen enthalten (z. B. Auszüge aus der Brandschutzordnung, Übungsplanung, Maßnahmenbeschreibungen, etc.)

Mittels Dokumentation klare Vorgaben schaffen

Ein IT-Notfallhandbuch ist das zentrale Mittel in der IT-Notfallbewältigung!

Klares Layout

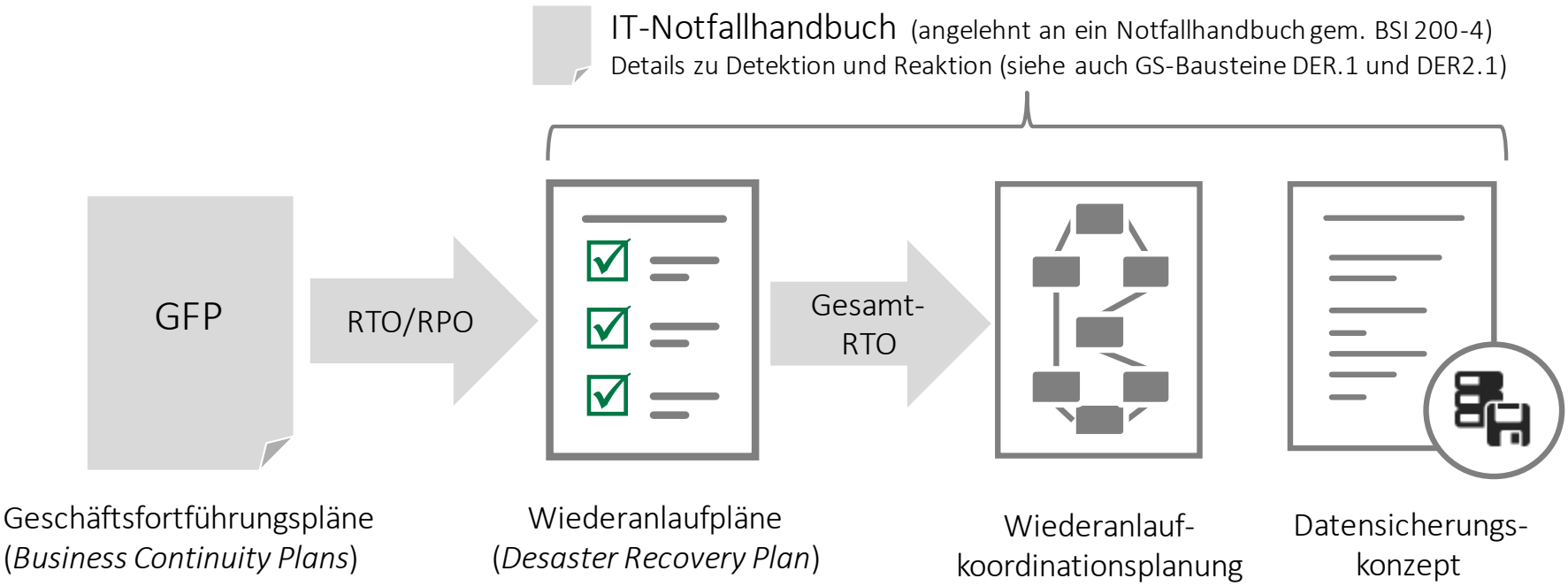
Keine „Prosa“

Checklisten-basiert

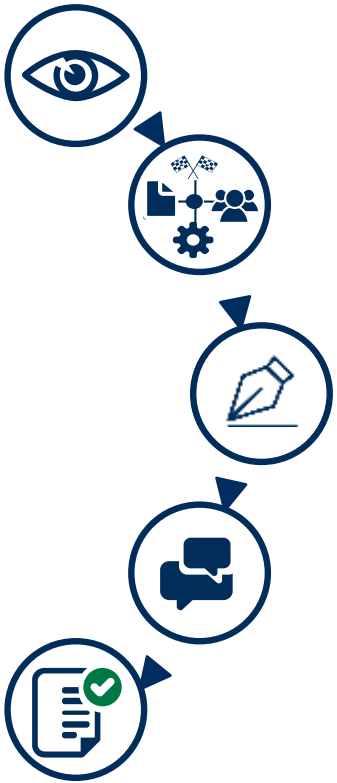
Es umfasst u. a. folgende Inhalte:

- Verfahren zu Meldung, Alarmierung und Eskalation
- Übergreifende Vorgaben zur Zusammensetzung der Notfallorganisation (insb. zum Krisenstab)
- Szenario-spezifische Checklisten, Templates (z. B. Protokollvorlage, Agenda für Lagebesprechungen, etc.) und Hilfsmittel (z. B. zum Maßnahmentracking, Rollenkarten)

How To | IT-Notfalldokumentation



How-To | IT-Wiederanlaufplanung



Empfohlene Mindestinhalte (Auswahl):

- Technische und organisatorische Voraussetzungen zum Wiederanlauf der Ressource
- Durchzuführende Aktivitäten zum Wiederanlauf
- Beschreibung von Funktionstests und der Übergabe in den Notbetrieb
- Notbetrieb und zu erwartende Einschränkungen
- Maßnahmen zur Rückführung in den Normalbetrieb

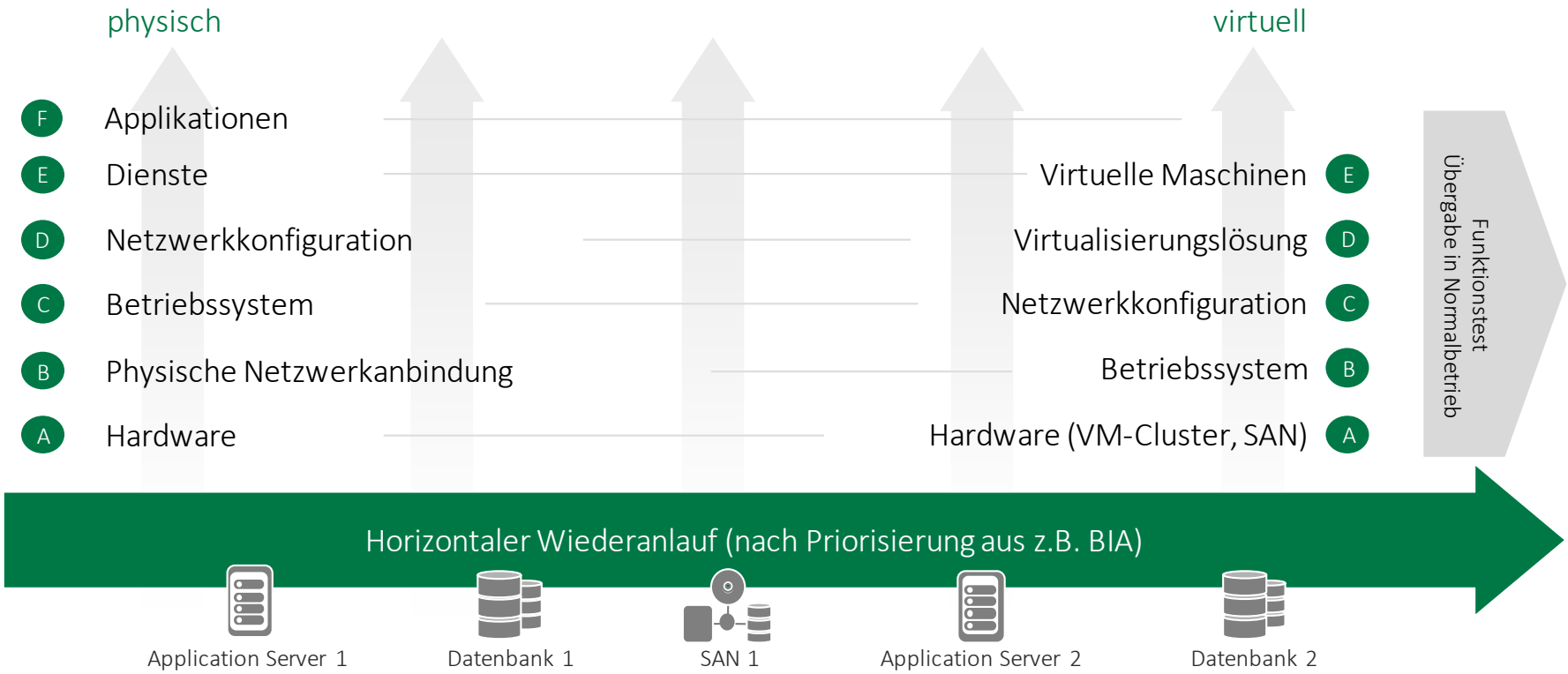
Exkurs: Beispielinhalte eines IT-Wiederanlaufplans

Exkurs

Bundesamt
für Sicherheit in der
Informationstechnik

BSI Standard 200-4

Wiederanlaufpläne beschreiben vertikalen Wiederanlauf

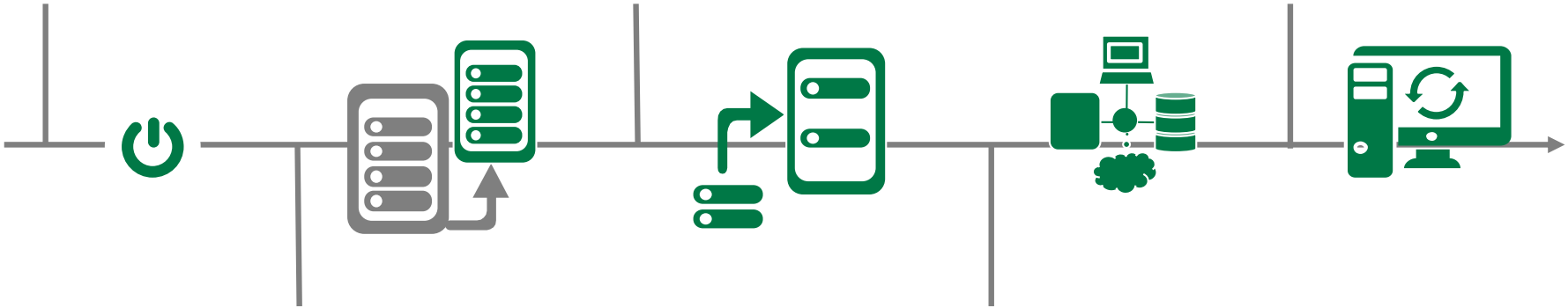


Beispiel | Prozedur eines Wiederanlaufs | 1/2

Prüfen des Produktionsstatus
Ggf. Deaktivieren von noch laufenden Applikationen, DB, etc.

Datensicherungen
(Server / OS) zur Verfügung stellen

Installation / Anpassung Middleware
DBMS, Batch-Steuerung, Überwachung, Connectivity, usw.



Bereitstellung Ausweich-Hardware
Server und Storage

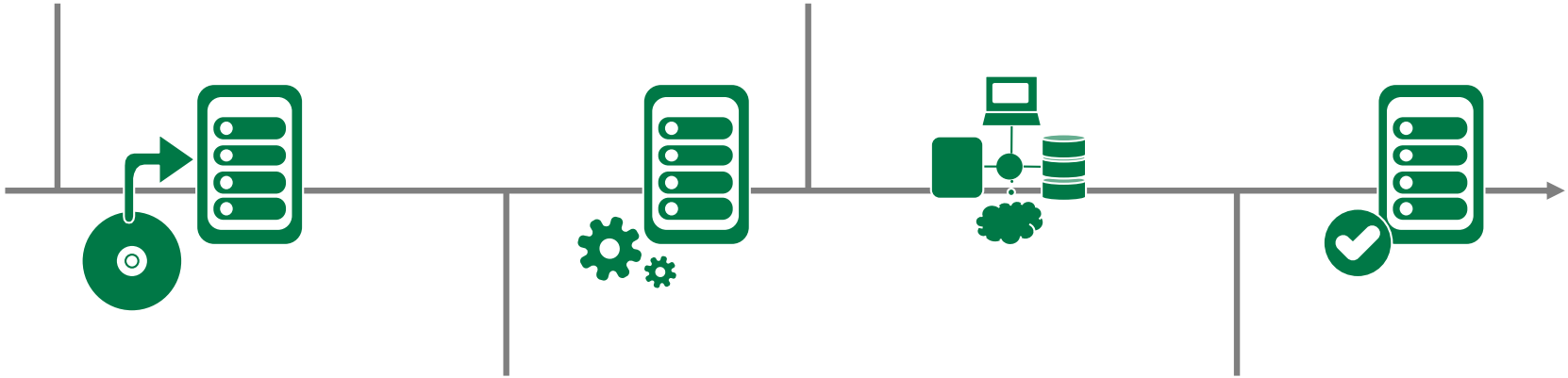
Installation
Betriebssystem Konfiguration
Netzanbindung

Beispiel | Prozedur eines Wiederanlaufs | 2/2

Bereitstellung der Anwendungsdaten

(z. B. Tape to Disk)

Schnittstellen konnektieren



Recovery von Anwendungsdaten

DB-Recovery

Systemcheck und Übergabe

Schwimmweste tragen → Überlebensvoraussetzungen

Erschaffen Sie eine Grüne Zone

- Halten Sie wichtige Hardware oder Systeme vor, um in den ersten Tagen der Krise wertvolle Zeit zu sparen:
  - Benutzermanagement, in welchem Sie kurzfristig Key-User anlegen können
  - Kommunikationslösung (Azure / AWS), um ihre E-Mail Kommunikation schnell etablieren zu können
  - Laptops, auf denen die Wiederanlaufplanung verfügbar ist

Etablieren Sie eine sicherheitsrelevante Systemprotokollierung von Ereignissen

- An- und Abmeldevorgänge
- Änderungen an Sicherheits- und Protokollierungseinstellungen
- Änderungen in der Berechtigungsverwaltung

Bilden Sie Redundanzen

- Kontaktdaten, Kommunikationswege oder auch für ganze System. Dies kann zum Beispiel durch eine Cloud-Notfallumgebung realisiert werden.

Wrap Up | Best Practices: Präventionsmaßnahmen für **Ausfall von IT-Komponenten**

- Eigene Lösung: Redundanz
  - Hochverfügbarkeit oder Hot-Standby (Verteilte Systeme / Cluster)
  - Warm-Standby (Systeme vorhanden, müssen noch aktiviert werden)
  - Cold-Standby (nur Fläche und Leitungen)
- Cloud-Dienste
- Einsatz von Hosting-Dienstleistern
- Wiederbeschaffung/-aufbau

Faktor Backups

Anforderungen

- Kein Zugriff der zu sichernden Systeme auf die Daten
- Daten dürfen nicht mit Domänenberechtigungen erreichbar sein
- Daten dürfen nicht mit den selben Kennwörtern erreichbar sein, die auch in der Domäne verwendet werden.

Lösungen

- Klassische Offline-Backups wie externe Festplatten, Tapes oder WORM-Medien
- Pull-Verfahren durch Backup Server oder NAS-Systeme
- NAS-Snapshots
- Oder: Cloud-Backups

Vergessen Sie nicht die Funktionalität ihrer Backups mit einem Wiederherstellungstest zu überprüfen!

…und wenn´s doch mal kracht: Wiederanlaufpläne ausgelagert sichern!

Tragen Sie folgenden Leitspruch in Ihre Institution

> 5 minutes before party,
> it's not time to learn to dance.
>
> Snoopy

Unterschied: Testen und Üben

Tests: Prüfung konkreter Verfahren oder technischer Maßnahmen auf ihre Funktionsfähigkeit

- Startet die USV selbsttätig nach Ausfall der Hauptstromversorgung?
- Funktioniert das Zurückspielen von Datensicherungen auf den wiederhergestellten IT-Systemen?

Übungen: Durchspielen von Ausfall- bzw. Notfallszenarien, um Pläne oder Abläufe des (reaktiven) ITSCMs mit praktischer Beteiligung der Mitarbeiter zu überprüfen

- Können die im IT-Wiederherstellungsplan definierten RTO durch die Mitarbeiter realisiert werden?
- Funktionieren die im IT-Notfallhandbuch definierten Alarmierungs- und Meldewege?

Die meisten Unternehmen haben eine Versicherung…

…für Brandschutz und Betriebsunterbrechung, allerdings keine für Cyber

Dabei kann eine Cyberversicherungen im Notfall eine Pannenhilfe stellen

Achtung:

Eine Versicherung kann nur eine Ergänzung zur Prävention und kein Ersatz sein!

Fragen?


HISOLUTIONS
Schloßstraße 1 | 12163 Berlin
info@hisolutions.com | +49 30 533 289 0
www.hisolutions.com
Walther-Schreiber-Platz
© HiSolutions 2023