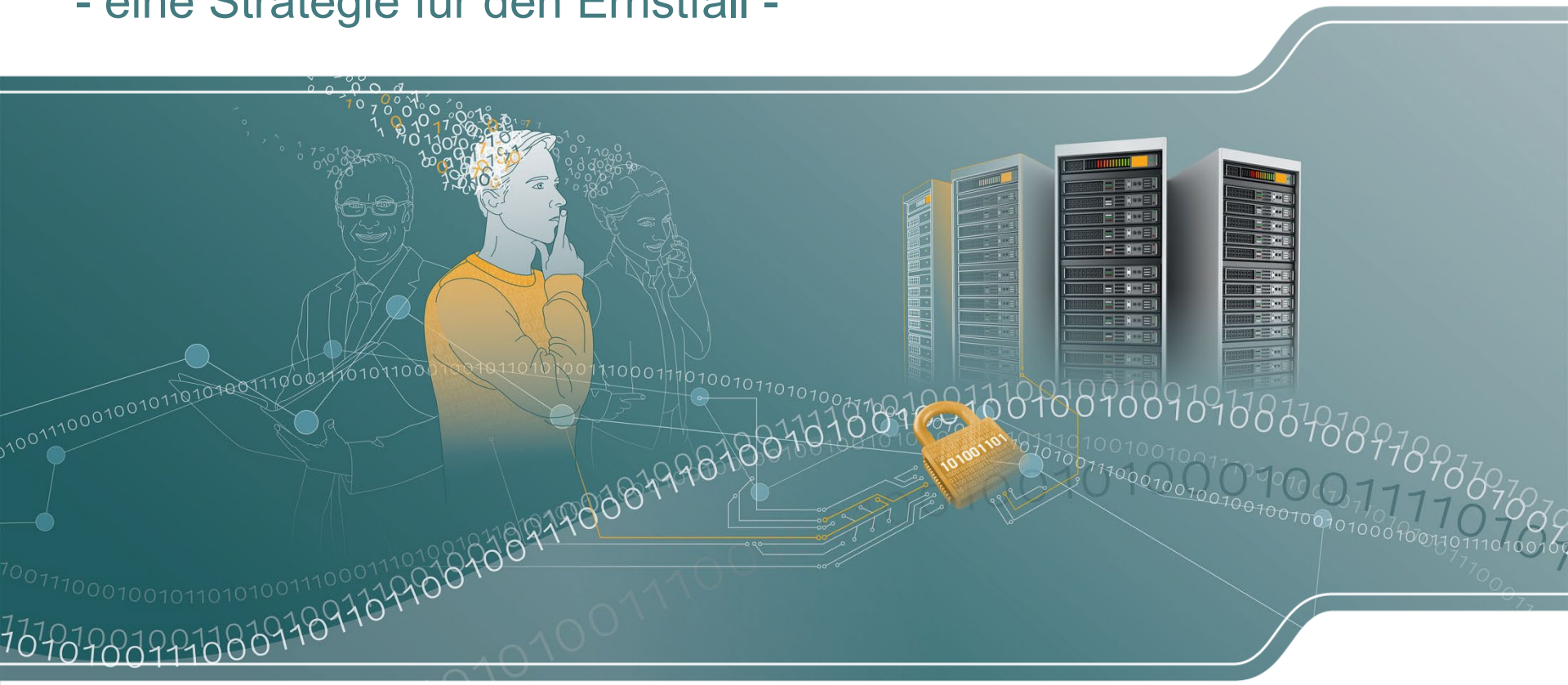
STAATSBETRIEB
SÄCHSISCHE
INFORMATIK DIENSTE

Freistaat
SACHSEN

Sicherheit im Chaos: IT-Notfallmanagement im Freistaat Sachsen

- eine Strategie für den Ernstfall -



Axel Geck - SID & Claudia Brückner - SK I V. Kundenforum des SID am 26. September 2023 im TSW Radebeul

IT-Notfallmanagement im Freistaat Sachsen

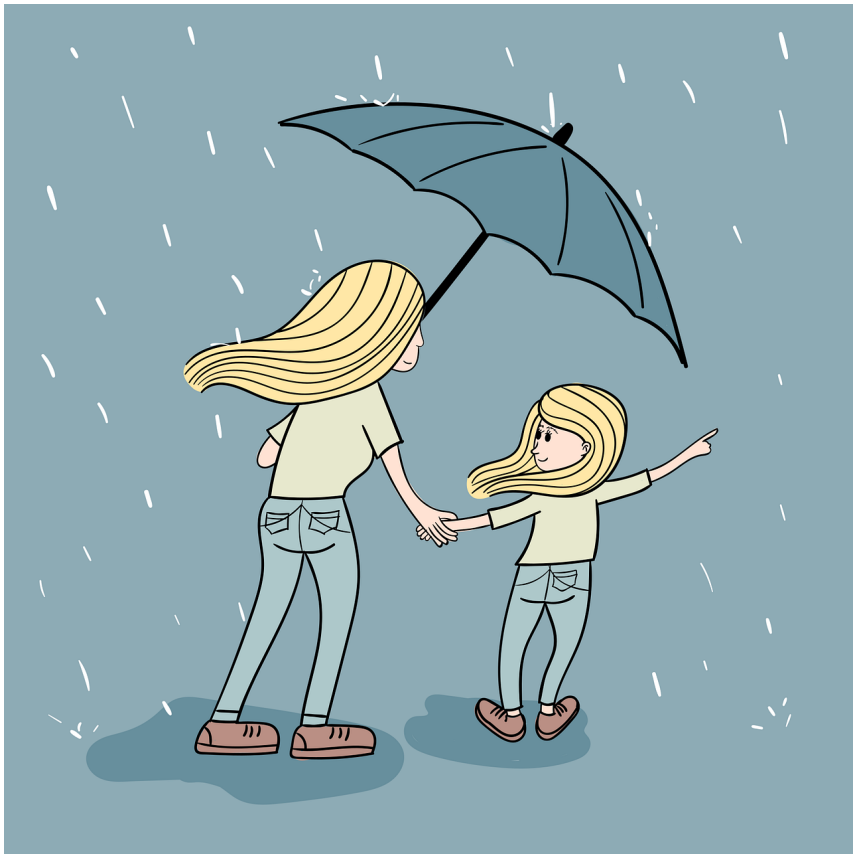
- Gliederung -

- warum ist ein IT-Notfall zu „managen“?
- Standort des IT-Notfallmanagements
- was ist ein IT-Notfall in Abgrenzung zu anderen Störereignissen?
- Ziele des Notfallmanagements

Das wollen wir vermeiden…

…aufgeregt umherirren und nicht wissen, was zu tun ist

Blick in die Zukunft …



- es handelt sich nicht um die Frage, ob ein IT-Notfall eintreten wird, sondern wann er eintreten wird
- daher geht es darum, auf die Zukunft vorbereitet zu sein und Resilienz zu trainieren

Ziele des IT-Notfallmanagements

- Schaffung von Widerstandsfähigkeit (Resilienz) gegenüber Schadensereignissen
- ein Baustein in der Resilienz: Aufbau eines IT Notfallmanagementsystems als fortlaufender Prozess

Ziele des IT-Notfallmanagements

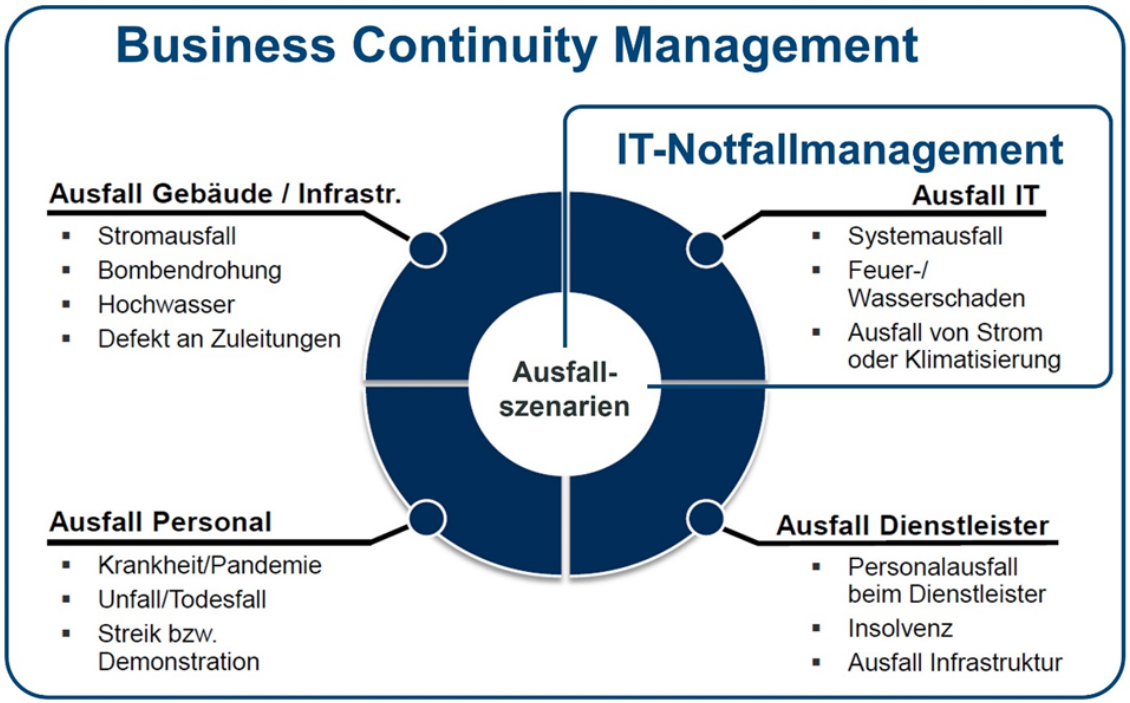
Ziel ist es sicherzustellen, dass

- wichtige Geschäftsprozesse selbst in kritischen Situationen nicht oder nur temporär unterbrochen werden und
- die Institution auch bei einem größeren Schadensereignis handlungsfähig bleibt.

IT-Notfallmanagement als Bestandteil

des Business Continuity Managements (BCM)

- BSI-Standard 200-4: Business Continuity Management
- im IT-NM begrenzt sich das Erkennen von Risiken und deren Behandlung auf IT-bezogene Verfahren und darin genutzte IT-Ressourcen
- im IT-NM werden keine Parallelstrukturen zum BCM aufgebaut

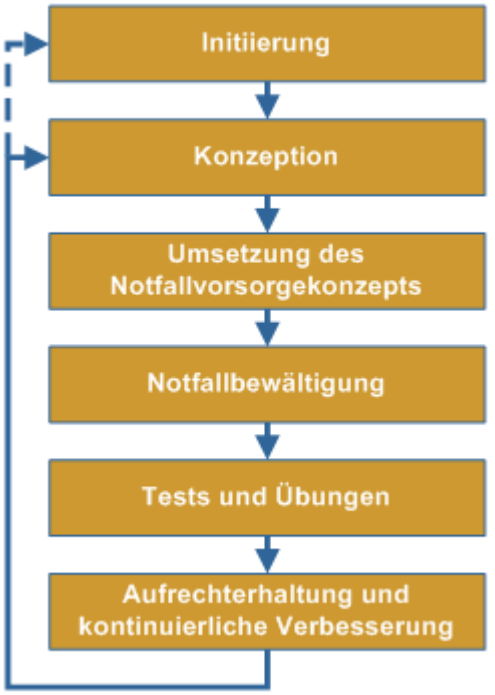


Vorgehen im IT-Notfallmanagement

1. Leitlinie zum IT-Notfallmanagement definieren
2. Verantwortlichkeiten für IT-Notfallmanagement festlegen
3. Organisation und Geschäftsprozesse analysieren
4. IT-Systeme und Kommunikationswege dokumentieren
5. Externe Unterstützung (z. B. IT-Dienstleister) einholen
6. Vorsorgekonzept erstellen
7. Notfallhandbuch erstellen

Dokumentation

8. Kommunikation festlegen
9. Üben und Schulen
10. Lehren aus IT-Notfällen ziehen

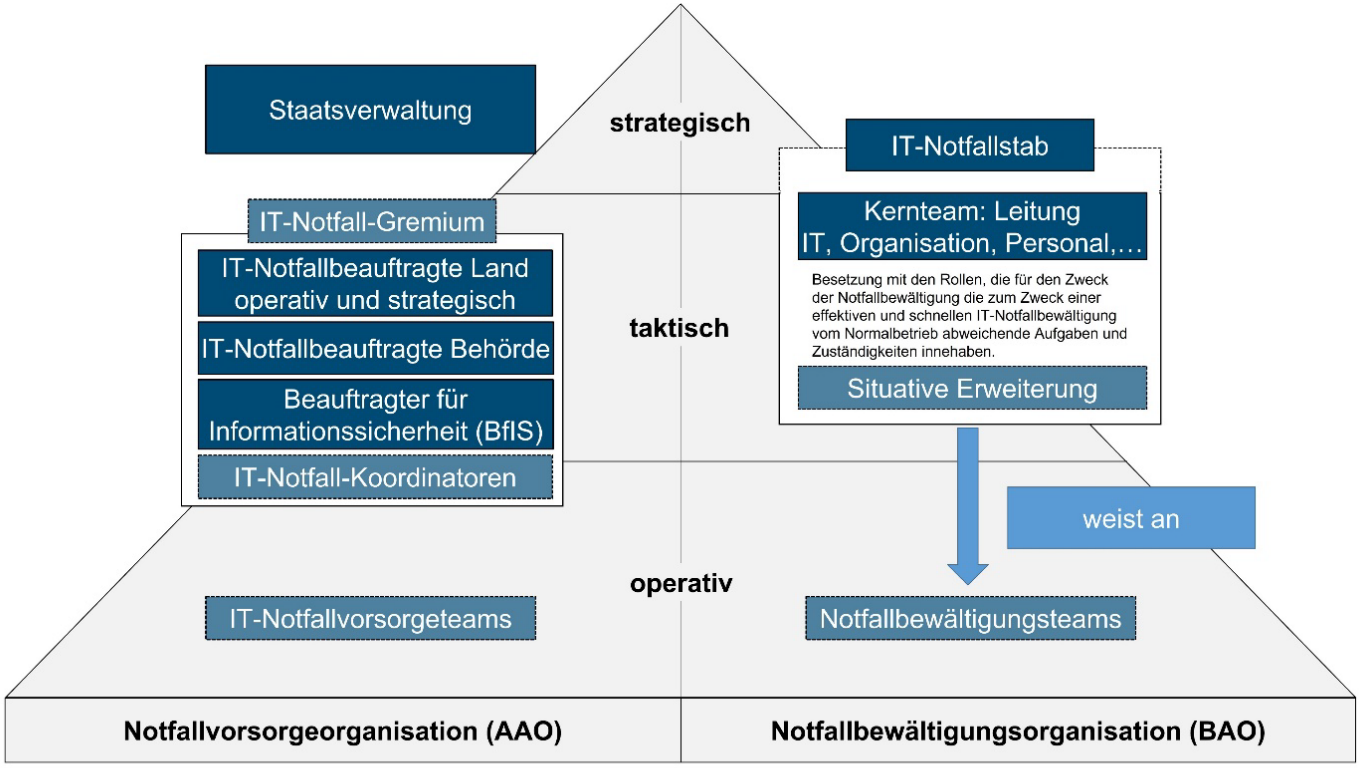


Quelle: BSI - 1.6 Notfallmanagement-Prozess (bund.de)

Leitlinie zum IT-Notfallmanagement

- Geltungsbereich
- Stellenwert und Zielsetzung
- Kernaussagen der IT-Notfallstrategie
- Vorgehensmodell
- Struktur der Aufbauorganisation
- Verpflichtung der Optimierung des IT-Notfallmanagements
- Gesetze, Richtlinien und Vorschriften
- Definition zentraler Begriffe
- Übernahme der Gesamtverantwortung durch die Leitung

Verantwortlichkeiten für IT-Notfallmanagement
- Aufbauorganisation in der Sächsischen Staatsverwaltung -



Verantwortlichkeiten für IT-Notfallmanagement
- IT-Notfallvorsorgeorganisation (AAO) -

Rollen und Aufgaben im IT-Notfallmanagement:

- Beauftragten für Informationstechnologie des Freistaates Sachsen (CIO)

  → verantwortlich für die behördenübergreifende Sicherstellung des IT-Notfallmanagement in der Staatsverwaltung

- Strategischen IT-Notfallbeauftragten (Land)

  → zuständig für die strategische Ausrichtung des IT-Notfall-managements und für die Umsetzung des IT-Notfallmanagement-systems auf Landesebene

Verantwortlichkeiten für IT-Notfallmanagement
- IT-Notfallvorsorgeorganisation (AAO) -

Rollen und Aufgaben im IT-Notfallmanagement:

- Operativen IT-Notfallbeauftragten (Land)

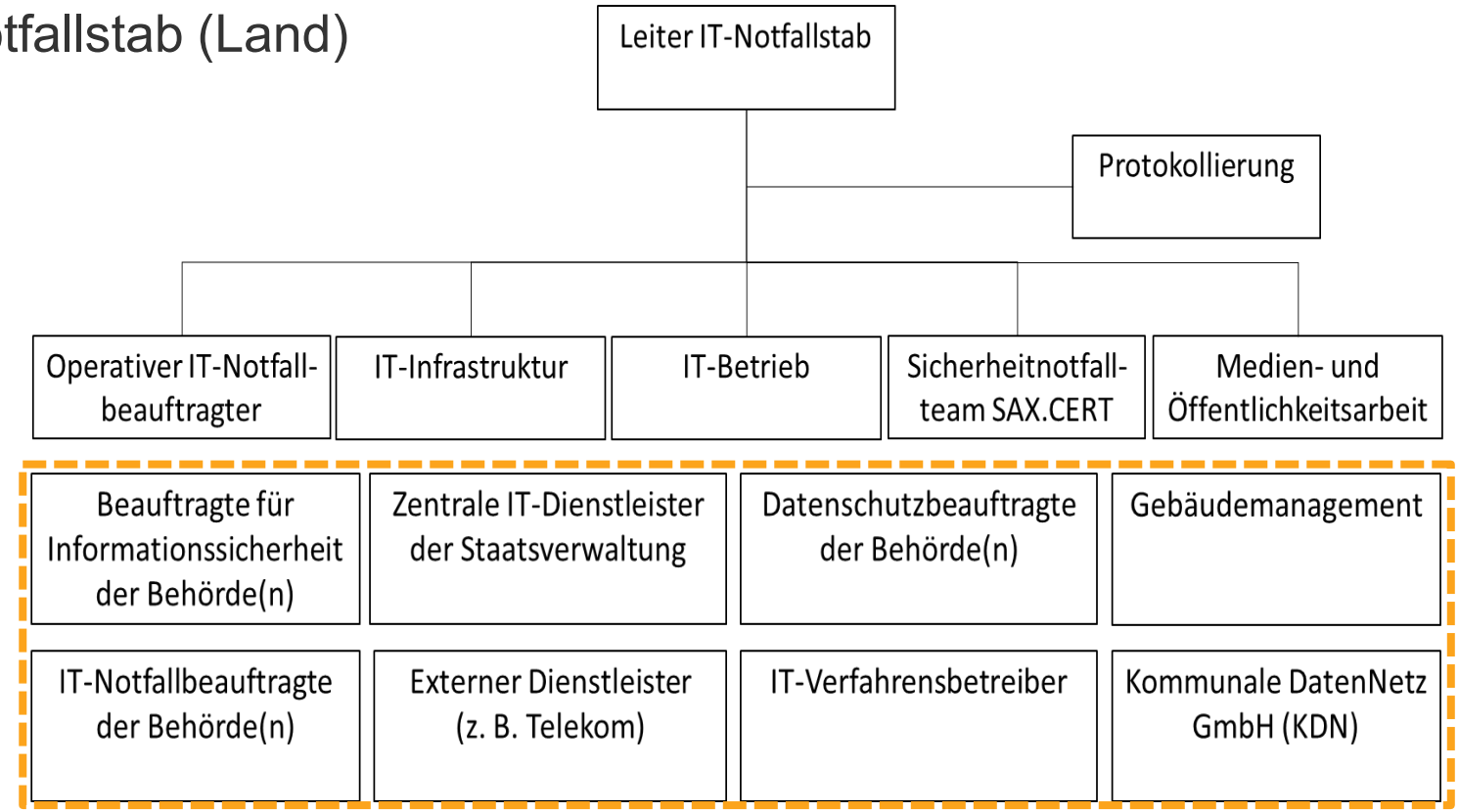
  → steuert alle Aktivitäten rund um die Notfallvorsorge und wirkt bei den damit verbundenen Aufgaben mit

- IT-Notfallbeauftragten der wesentlichen Behörden der Staatsverwaltung nach § 7 Abs. 1 SächsISichG

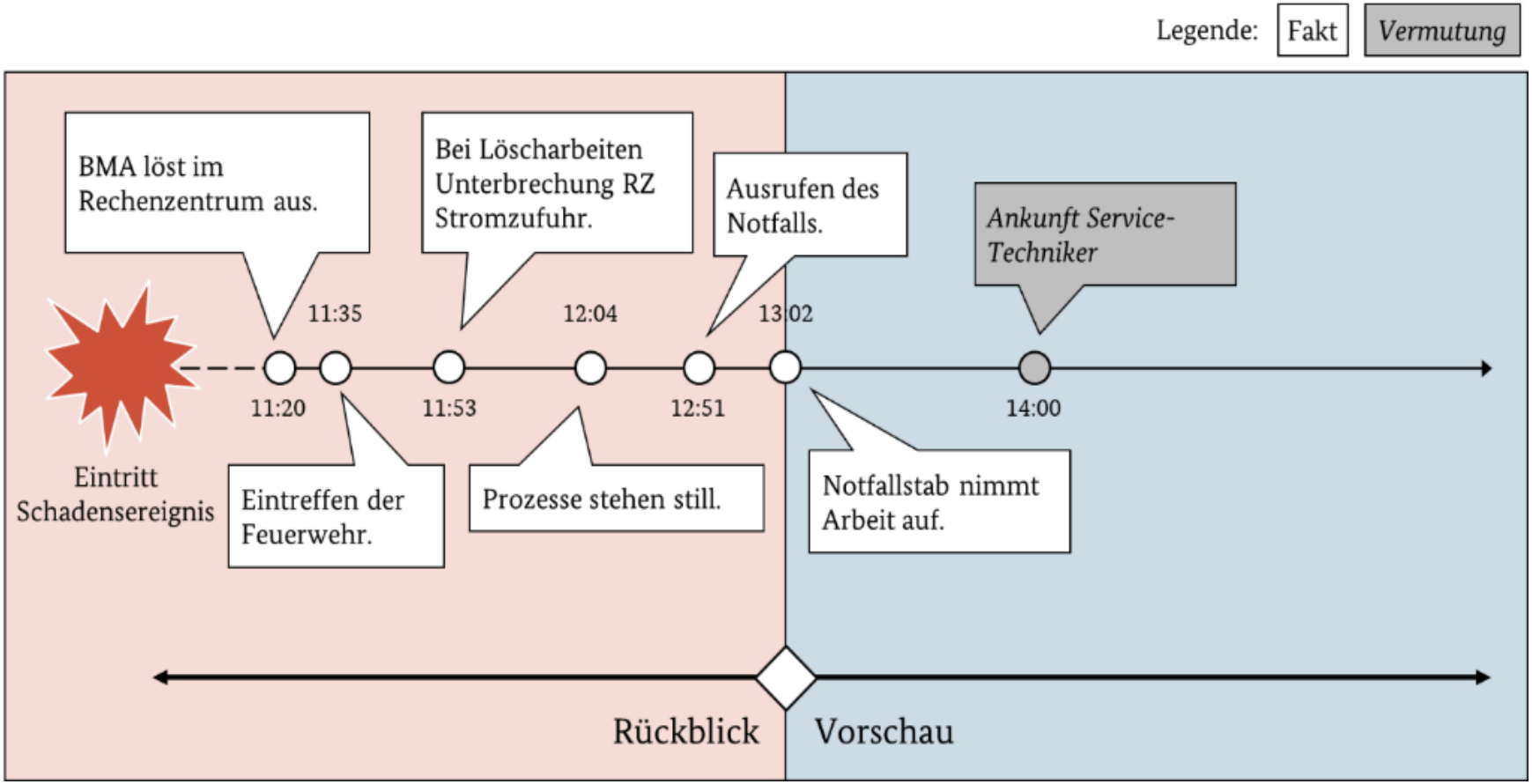
  → steuern alle Aktivitäten rund um die Notfallvorsorge und wirken bei den damit verbundenen Aufgaben mit

Verantwortlichkeiten für IT-Notfallmanagement
- IT-Notfallbewältigungsorganisation (BAO) -

IT-Notfallstab (Land)



Lagebeobachtung und -visualisierung



Quelle: BSI-Standard 200-4 BCM (bund.de)

Verantwortlichkeiten für IT-Notfallmanagement
- IT-Notfallbewältigungsorganisation (BAO) -

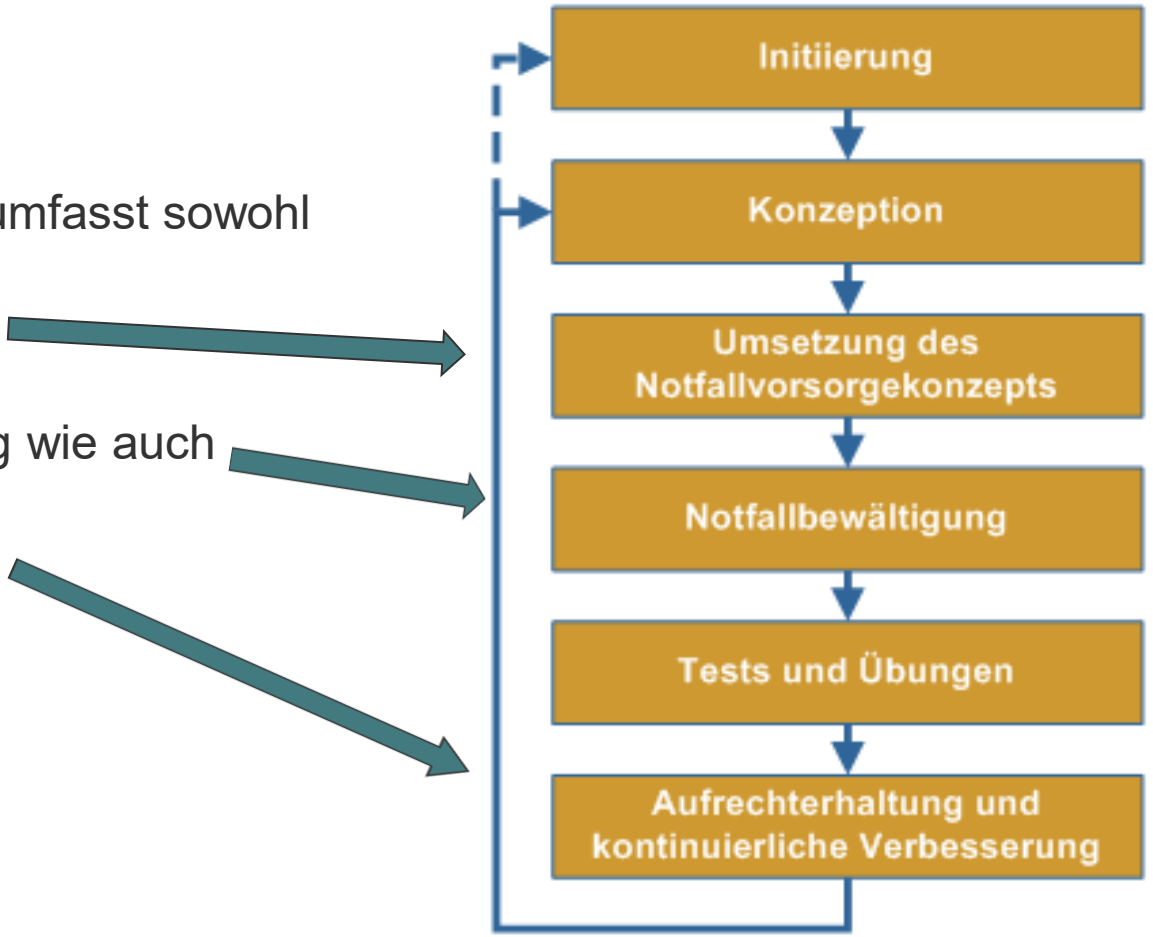
IT-Notfallstab (Land)

- Richtlinie zum IT-Notfallstab
  - Organisation des IT-Notfallstabes
  - Vorgehen beim Ausrufen eines IT-Notfalls
  - Konstituierung und Auflösung des IT-Notfallstabes
  - Festlegungen für den IT-Notfallstab
  - Handlungsbefugnisse des IT-Notfallstabes
  - Regeln für die Stabsarbeit
  - Aufwuchs zur IT-Krise und Schnittstellen zum Verwaltungsstab

Vorgehen im IT-Notfallmanagement

Ein IT-Notfallmanagement umfasst sowohl

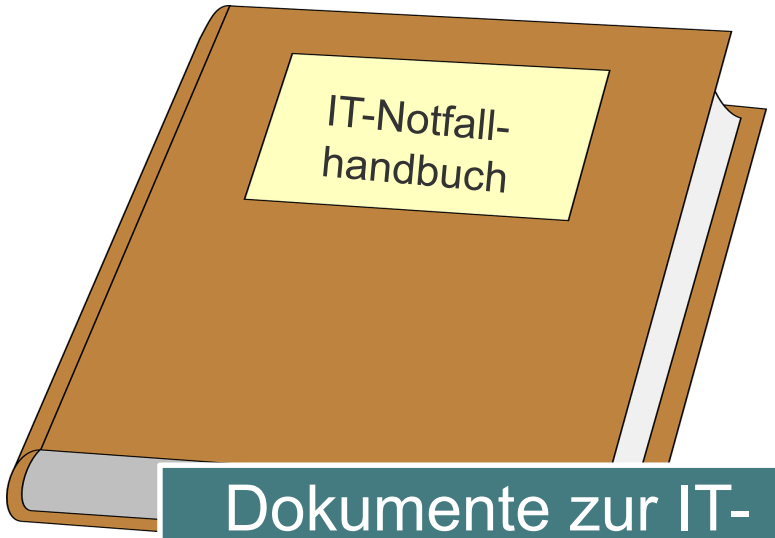
- die IT-Notfallvorsorge,
- die IT-Notfallbewältigung wie auch
- die IT-Notfallnachsorge.



STAATSBETRIEB SÄCHSISCHE INFORMATIK DIENSTE | Freistaat SACHSEN

IT-Notfallmanagement – Dokumentenstruktur

Dokumente zur IT-Notfallvorsorge



Dokumente zur IT-Notfallbewältigung

STAATSBETRIEB SÄCHSISCHE INFORMATIK DIENSTE | Freistaat SACHSEN

IT-Notfallmanagement – Dokumentation

STAATSBETRIEB
SÄCHSISCHE
INFORMATIK DIENSTE

Freistaat
SACHSEN

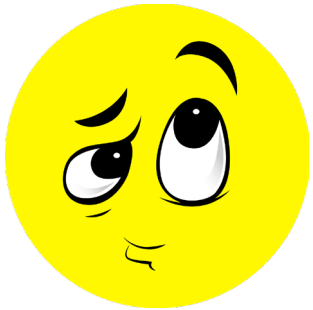
IT-Notfallmanagement – Dokumentation

IT-Notfallhandbuch

- Geschäftsfortführungspläne
- Wiederanlaufpläne
- Wiederherstellungspläne
- Geschäftsordnung des Stabes
- Kommunikationskonzept
- …

IT-Notfallmanagement – Dokumentation

- Was dokumentieren? Mögliche IT-Notfallszenarien überlegen …
  - Server- oder Netzwerkausfall
  - Ausfall der Kommunikationsinfrastruktur (E-Mail, VoIP, …)
  - Datenverlust oder Datenmanipulation
  - Schwachstellen in Hard- oder Software
  - …



IT-Notfallmanagement – Dokumentation

- Wie dokumentieren? IT-Notfallplan entwickeln …

Notfallvorsorge	Notfallbewältigung
Notfallteam und Verantwortlichkeiten festlegen	Notfallteam für Notfallbewältigung informieren
Notfallkontaktliste erstellen →	
Eskalationsstrategien definieren Externe IT-Sicherheitsexperten hinterlegen →	Sachstand erfassen: - Schwere des IT-Notfalls bewerten - betroffene IT-Systeme bzw. IT-Verfahren und Ursache ermitteln
Interessensgruppen ermitteln, Kommunikationsstrategie planen und Kommunikationskonzept erstellen →	Kommunikationskonzept umsetzen

Dokumentation

STAATSBETRIEB SÄCHSISCHE INFORMATIK DIENSTE | Freistaat SACHSEN

IT-Notfallmanagement – Dokumentation

- Wie dokumentieren? IT-Notfallplan entwickeln …

Notfallvorsorge	Notfallbewältigung
detaillierten Wiederherstellungsplan beschreiben	Wiederherstellungsprozess initiieren und prüfen
Sicherheitsmaßnahmen implementieren	Ursachenanalyse durchführen
Schulungen und Übungen durchführen	Bericht erstellen; Nachbesprechung durchführen; Verbesserungspotenziale ermitteln
IT-Notfallplan aktualisieren	

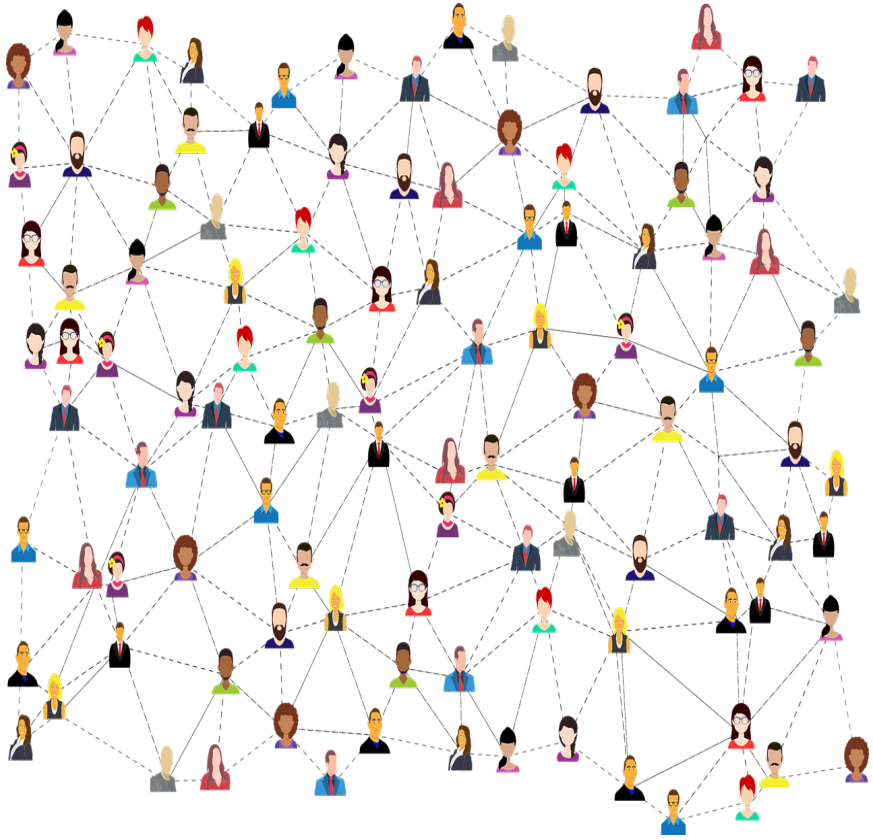
Dokumentation

STAATSBETRIEB
SÄCHSISCHE
INFORMATIK DIENSTE

Freistaat
SACHSEN

IT-Notfallmanagement – Kommunikation

- Reihenfolge in der IT-Notfall-Kommunikation
  - Feststellender eines Sicherheitsvorfalls → Meldung an zentrale Meldestelle
  - Leitungsebene → Kenntnis vom Sicherheitsvorfall + ggf. Abschaltung der Systeme
  - Managementebene → Information an Mitarbeiter
  - Interne IT-Mitarbeiter → Sachstandsermittlung



IT-Notfallmanagement – Kommunikation

- Reihenfolge in der IT-Notfall-Kommunikation

- Besondere Aufbauorganisation → Notfallstab + Notfallbewältigung aktivieren
  - BfIS → BSI / ZAC informieren
  - ??? → externe IT-Unterstützung organisieren
  - ??? → Forensiker bzw. IT-Sicherheitsexperte bestellen
  - ??? → Notfall-Webseite starten – zeitversetzte Information der Öffentlichkeit
  - ??? → Datenschutzbeauftragte benachrichtigen

- IT-Notfall-Kommunikation
  - Ausweichkommunikation (z. B. Signal) festlegen
  - Regelungen zur Kommunikation (z. B. nur PuÖ kommuniziert nach außen)

STAATSBETRIEB
SÄCHSISCHE
INFORMATIK DIENSTE

Freistaat
SACHSEN

IT-Notfallmanagement – Kommunikation

- Leitungsebene
- Interne Beschäftigte
- Beschäftigte im IT-Bereich
- Inanspruchnehmer von Verwaltungsleistungen
- Öffentlichkeit
- Medienvertreter
- Polizei
- Aufsichtsbehörde
- …

STAATSBETRIEB
SÄCHSISCHE
INFORMATIK DIENSTE

Freistaat
SACHSEN

Erfahren Sie mehr…

Sie finden uns unter:
www.sid.sachsen.de

Dresdner Straße 78 A
01445 Radebeul
Telefon 0351 3264 5101
poststelle@sachsen.de