NOTFALLMANAGEMENT IN DER INFORMATIONSTECHNIK

BSI-STANDARD 200-4 BUSINESS CONTINUITY MANAGEMENT IN DER PRAXIS

Mediaserver Hamburg / Maxim Schulz

06.01.2026 | Olaf Moser, ISB

LSBG
Landesbetrieb Straßen, Brücken und Gewässer Hamburg

Hamburg

AGENDA

01 Vorstellung LSBG

02 Was ist Notfallmanagement?

03 Vorstellung des BSI 200-4 Business Continuity Management

04 Praktische Realisierung des BCM

05 Erfahrungen mit IT-Notfällen

06 Was kann denn schon geschehen?

07 Was kann ich machen?

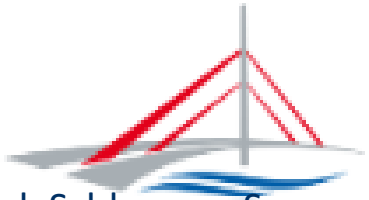
VORSTELLUNG LSBG

01

VORSTELLUNG LSBG

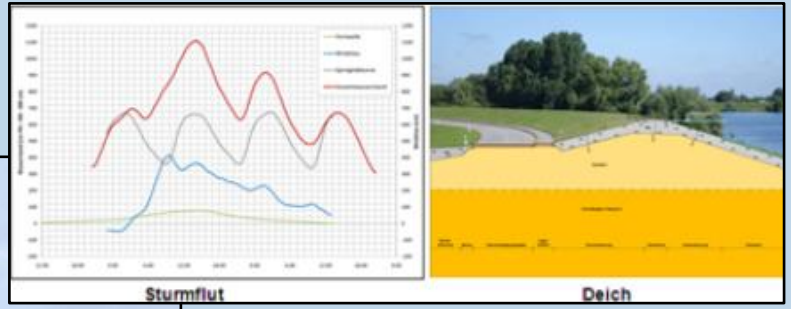
Der LSBG plant, baut, erhält einen Großteil der Hamburger Verkehrsinfrastruktur und verantwortet deren gesamten Life-Cycle

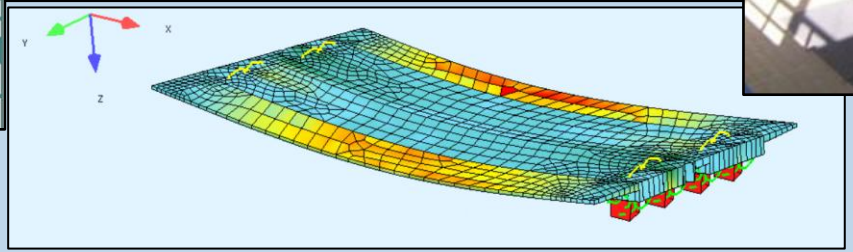
- Hauptverkehrsstraßen
- Binnen- und Küstenhochwasserschutz
- Gewässer (außer Bundeswasserstraßen)
- Konstruktive Bauwerke (u.a. Brücken, Tunnel, Schleusen, Sperr- und Schöpfwerke)
- Lichtsignal- und Verkehrstelematikanlagen



LSBG
Landesbetrieb Straßen, Brücken und Gewässer Hamburg

VORSTELLUNG LSBG





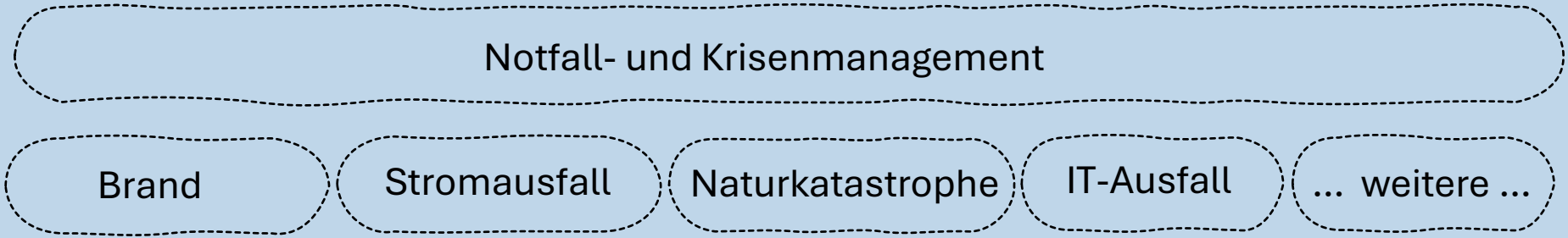
Hamburg

WAS IST NOTFALLMANAGEMENT?

02

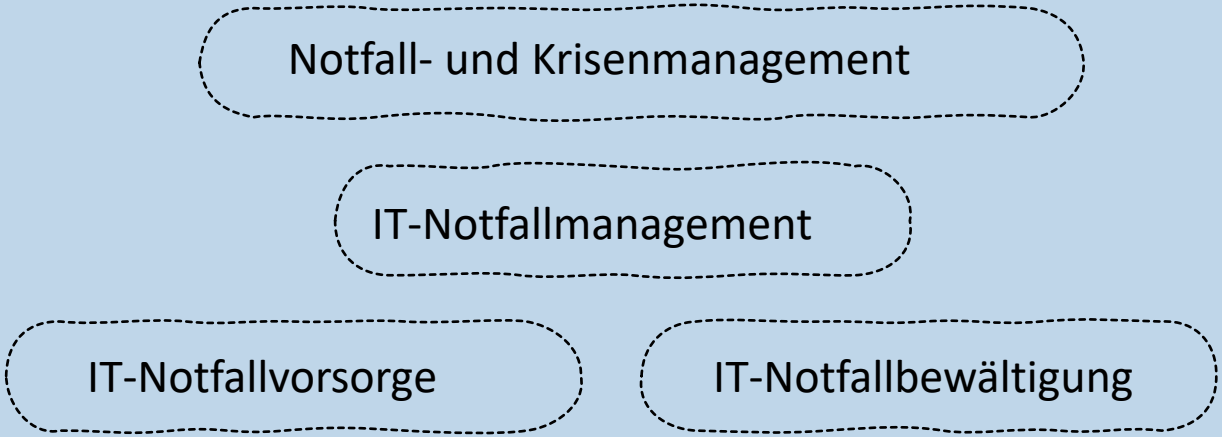
WAS IST NOTFALLMANAGEMENT?

Das Notfallmanagement befasst sich mit der Bewältigung von Störungen, die den Geschäftsbetrieb beeinträchtigen



WAS IST NOTFALLMANAGEMENT?

Das Notfallmanagement befasst sich mit der Bewältigung von Störungen, die den Geschäftsbetrieb beeinträchtigen



VORSTELLUNG DES STANDARDS BSI 200-4 BUSINESS CONTINUITY MANAGEMENT (BCM)

03

VORSTELLUNG DES BSI 200-4 BCM

- Das Notfallmanagement nach BSI 200-4 ist ein strategischer Prozess zur Sicherstellung der Handlungsfähigkeit bei IT-Notfällen, Störungen und Krisen
- Ziel ist die Erhöhung der Resilienz kritischer Geschäftsprozesse zur Gewährleistung der Fortführung unternehmenskritischer Verfahren
- Umfasst systematische Planung, Organisation und Kontrolle von Maßnahmen zur Notfall- und Krisenbewältigung
- Zu erreichendes Schutzziel -> Verfügbarkeit

BSI-Standard 200-4
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-4-Business-Continuity-Management/bsi-standard-200-4_Business_Continuity_Management_node.html

PRAKTISCHE REALISIERUNG DES BCM

04

PRAKTISCHE REALISIERUNG DES BCM

EINIGE WESENTLICHE ELEMENTE

Geschäftskritische Verfahren und Prozesse

- Benennung IT-Notfallbeauftragte:r
- Identifikation unternehmenskritischer Prozesse -> Kronjuwelen
- Identifikation deren IT-Verfahren + Systeme
- Wiederherstellungsanlaufpläne mit Priorisierung des Wiederanlauf von Verfahren
- Leitlinie, Notfallhandbuch, Eskalations- + Alarmierungspläne, Notfallkommunikation, Krisenstab, Dienstleister, …
- Es gilt: üben, üben, üben

Länderübergreifende Krisenmanagementübung (LÜKEX)
LÜKEX 2023 stellte ein massiver Cyberangriff das Regierungshandeln auf die Probe
LÜKEX 2011 haben Bund, Länder und weitere Akteure das Verhalten bei einer IT-Bedrohungslage geübt
https://www.bmi.bund.de/DE/themen/bevoelkerungsschutz/krisenmanagement/luekex/luekex-node.html

ERFAHRUNGEN MIT IT-NOTFÄLLEN

05

ERFAHRUNGEN MIT IT-NOTFÄLLEN

Einige Beispiele

- Das Annehmen des IT-Notfalls kann Tage andauern (Schockstarre)
- Aktuelle Liste der Notfallkontakte muss ausgedruckt vorhanden sein
- Unternehmenskritischen Prozesse müssen benannt sein
- Sofortiges Einbinden der Unternehmenskommunikation für in- und externe Kommunikation
- Fragen der Mitarbeitenden und Externen müssen beantwortet werden, zB wann werden wir wieder arbeiten können? werden Gehälter ausgezahlt?
- Wiederanlaufliste mit Priorisierung muss vorhanden sein
- Backups müssen vorhanden sein (Backup von vor der Kompromittierung)
- Es ist unklar, wer die Lage führt und welche Personalressourcen benötigt werden
- Es ist nicht klar, dass die intensive Bearbeitung Tage->Monate andauern kann
- Es werden viele Personalressourcen über lange Zeiträume gebunden (Personalvertretung)
- Es muss klar sein, wer unterstützen kann, evtl. bereits vorhandener Abrufvertrag
- Es sind rasch unterschiedliche Beschaffungsprozesse einzuleiten, zB externe Experten für allgemeine Unterstützung, Incidentbehandlung sowie Forensik, HW/SW, Verpflegung, Hotelbuchungen
- Konfigurierte und einsatzbereite NBs für Führungs-/Funktionskräfte müssen vorhanden sein
- SW/HW für das Notnetz muss vorhanden sein oder rasch beschafft werden

ERFAHRUNGEN MIT IT-NOTFÄLLEN

- Aktuelle Liste der Notfallkontakte muss ausgedruckt vorhanden sein
- Unternehmenskritischen Prozesse müssen benannt sein
- Sofortiges Einbinden der Unternehmenskommunikation für in- und externe Kommunikation
- Fragen der Mitarbeitenden und Externen müssen beantwortet werden, zB wann werden wir wieder arbeiten können? werden Gehälter ausgezahlt?
- Wiederanlaufliste mit Priorisierung muss vorhanden sein

Das Annehmen des IT-Notfalls kann Tage andauern (Schockstarre)

- Backups müssen vorhanden sein (Backup von vor der Kompromittierung)
- Es ist unklar, wer die Lage führt und welche Personalressourcen benötigt werden
- Es ist nicht klar, dass die intensive Bearbeitung Tage->Monate andauern kann
- Es werden viele Personalressourcen über lange Zeiträume gebunden (Personalvertretung)
- Es muss klar sein, wer unterstützen kann, evtl. bereits vorhandener Abrufvertrag
- Es sind nach unterschiedliche Beschaffungsprozesse einzuleiten, zB externe Experten für allgemeine Unterstützung, Incidentbehandlung sowie Forensik, HW/SW, Verpflegung, Hotelbuchungen
- Konfigurierte und einsatzbereite NBs für Führungs-/Funktionskräfte müssen vorhanden sein
- SW/HW für das Notnetz muss vorhanden sein oder rasch beschafft werden

ERFAHRUNGEN MIT IT-NOTFÄLLEN

- Das Annehmen des IT-Notfalls kann Tage andauern (Schockstarre)
- Aktuelle Liste der Notfallkontakte muss ausgedruckt vorhanden sein
- Unternehmenskritischen Prozesse müssen bekannt sein
- Sofortiges Einbinden der Unternehmenskommunikation für in- und externe Kommunikation
- Wiederanlaufliste mit Priorisierung muss vorhanden sein

In- und externe Kommunikation

Fragen der Mitarbeitenden und Externen müssen beantwortet werden

zB wann werden wir wieder arbeiten können?

werden Gehälter ausgezahlt?

- Es ist unklar, wer die Lage führt und welche Personalressourcen benötigt werden
- Es ist nicht klar, dass die intensive Bearbeitung Tage->Monate andauern kann
- Es werden viele Personalressourcen über lange Zeiträume gebunden (Personalvertretung)
- Es muss klar sein, wer unterstützen kann, evtl. bereits vorhandener Abrufvertrag
- Es sind rasch unterschiedliche Beschaffungsprozesse einzuleiten, zB externe Experten für allgemeine Unterstützung, Incidentbehandlung sowie Forensik, HW/SW, Verpflegung, Hotelbuchungen

ERFAHRUNGEN MIT IT-NOTFÄLLEN

- Das Annehmen des IT-Notfalls kann Tage andauern (Schockstarre)
- Aktuelle Liste der Notfallkontakte muss ausgedruckt vorhanden sein
- Unternehmenskritischen Prozesse müssen bekannt sein
- Sofortiges Einbinden der Unternehmenskommunikation für in- und externe Kommunikation
- Wiederanlaufliste mit Priorisierung muss vorhanden sein

Backups

Backups müssen vorhanden sein

Wurde ein Restore eines Backups einmal erfolgreich durchgeführt?

Backup von vor der Kompromittierung?

- Es ist unklar, wer die Lage führt und welche Personalressourcen benötigt werden
- Es ist nicht klar, dass die intensive Bearbeitung Tage->Monate andauern kann
- Es werden viele Personalressourcen über lange Zeiträume gebunden (Personalvertretung)
- Es muss klar sein, wer unterstützen kann, evtl. bereits vorhandener Abrufvertrag
- Es sind rasch unterschiedliche Beschaffungsprozesse einzuleiten, zB externe Experten für allgemeine Unterstützung, Incidentbehandlung sowie Forensik, HW/SW, Verpflegung, Hotelbuchungen
- Konfigurierte und einsatzbereite NBs für Führungs-/Funktionskräfte müssen vorhanden sein

ERFAHRUNGEN MIT IT-NOTFÄLLEN

- Das Annehmen des IT-Notfalls kann Tage andauern (Schockstarre)
- Aktuelle Liste der Notfallkontakte muss ausgedruckt vorhanden sein
- Unternehmenskritischen Prozesse müssen bekannt sein
- Sofortiges Einbinden der Unternehmenskommunikation für in- und externe Kommunikation
- Fragen der Mitarbeitenden und Externen müssen beantwortet werden, zB wann werden wir wieder arbeiten können? werden Gehälter ausgezahlt?

Dauer

Es ist nicht klar, dass die intensive Bearbeitung Tage->Monate andauern kann

- Backups müssen vorhanden sein (Backup von vor der Kompromittierung)
- Es ist unklar, wer die Lage führt und welche Personalressourcen benötigt werden
- Es werden viele Personalressourcen über lange Zeiträume gebunden (Personalvertretung)
- Es muss klar sein, wer unterstützen kann, evtl. bereits vorhandener Abrufvertrag
- Es sind rasch unterschiedliche Beschaffungsprozesse einzuleiten, zB externe Experten für allgemeine Unterstützung, Incidentbehandlung sowie Forensik, HW/SW, Verpflegung, Hotelbuchungen
- Konfigurierte und einsatzbereite NBs für Führungs-/Funktionskräfte müssen vorhanden sein
- SW/HW für das Notnetz muss vorhanden sein oder rasch beschafft werden

WAS KANN DENN SCHON GESCHEHEN?

06

WAS KANN DENN SCHON GESCHEHEN?

DIE ZEIT

Hackerangriff

Landkreis ruft bundesweit ersten Cyber-Katastrophenfall aus

Ein Hackerangriff hat in Anhalt-Bitterfeld Teile der Verwaltung lahmgelegt. Sicherheitsbehörden vermuten einen Erpressungsversuch.

10. Juli 2021, 16:07 Uhr Quelle: DIE ZEIT, Reuters, ale

Ein Hackerangriff auf den Landkreis Anhalt-Bitterfeld hat den ersten Cyber-Katastrophenfall in Deutschland ausgelöst. Die Verwaltung des Landkreises in Sachsen-Anhalt muss nach eigenen Angaben fast zwei Wochen lang ihre Arbeit weitgehend einstellen, weil Kriminelle das Computersystem am 6. Juli attackiert haben.

Was ist passiert?

05.04.2023
Gruppe Royal spezialisiert auf Verschlüsselung von Microsoft- und Linux-Umgebungen

Erstmaßnahmen der ZBW (Auszug):

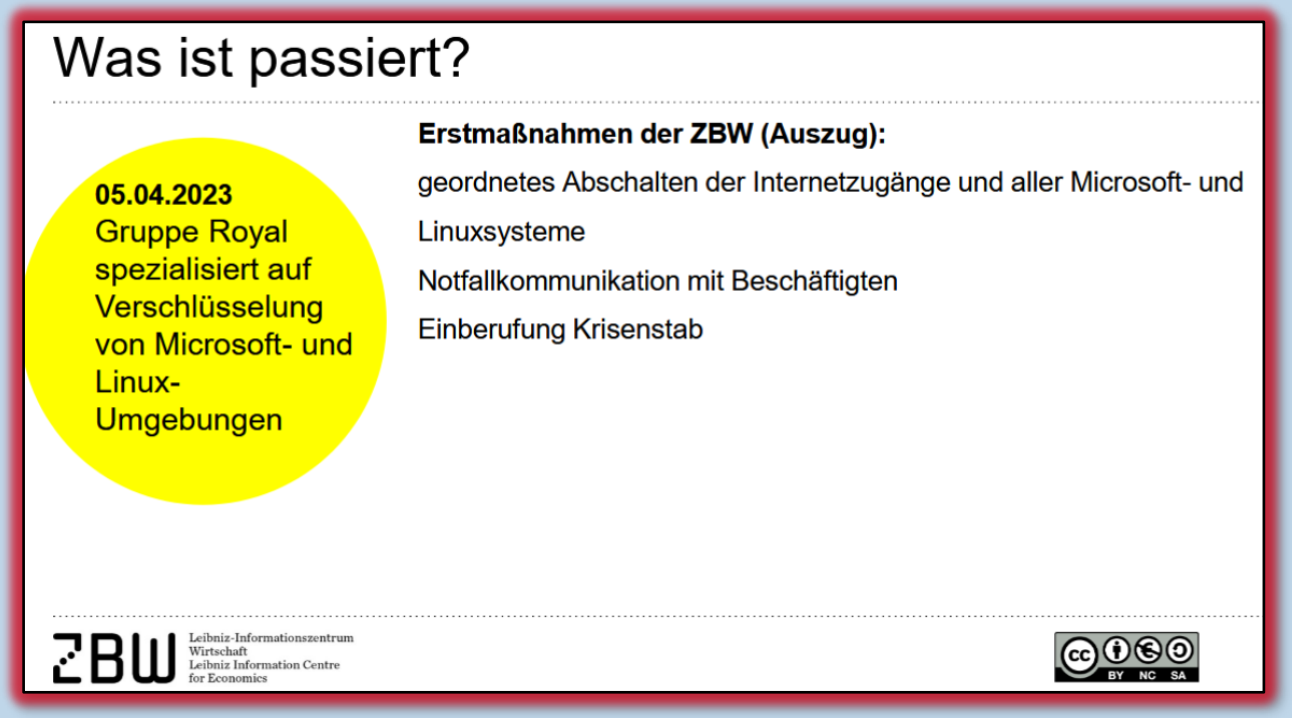
geordnetes Abschalten der Internetzugänge und aller Microsoft- und Linuxsysteme

Notfallkommunikation mit Beschäftigten

Einberufung Krisenstab

ZBW Leibniz-Informationszentrum Wirtschaft / Leibniz Information Centre for Economics

WAS KANN DENN SCHON GESCHEHEN?



https://www.langzeitarchivierung.de/Webs/nestor/SharedDocs/Downloads/DE/praesentationen/2023webseminarCyberAngriff.pdf?__blob=publicationFile&v=1

WAS KANN DENN SCHON GESCHEHEN?

DIE ZEIT

Hackerangriff

Landkreis ruft bundesweit ersten Cyber-Katastrophenfall aus

Ein Hackerangriff hat in Anhalt-Bitterfeld Teile der Verwaltung lahmgelegt. Sicherheitsbehörden vermuten einen Erpressungsversuch.

10. Juli 2021, 16:07 Uhr Quelle: DIE ZEIT, Reuters, ale

Ein Hackerangriff auf den Landkreis Anhalt-Bitterfeld hat den ersten Cyber-Katastrophenfall in Deutschland ausgelöst. Die Verwaltung des Landkreises in Sachsen-Anhalt muss nach eigenen Angaben fast zwei Wochen lang ihre Arbeit weitgehend einstellen, weil Kriminelle das Computersystem am 6. Juli attackiert haben.

https://www.mdr.de/mdr-sachsen-anhalt/podcast/you-are-fucked/index.html

KANN ICH AUCH SELBER BETROFFEN SEIN? OPFER WERDEN?

Patchday: Attacken auf Geräte mit Android 13, 14, 15 und 16 beobachtet

Google Android-Bugdroid vor Schloss-Symbol. (Bild: Primakov/Shutterstock.com)

02.12.2025, 10:59 Uhr Lesezeit: 2 Min. | Security

Mit wichtigem Sicherheitsupdate: macOS 15.3.2 und iOS 18.3.2 verfügbar

Apple hat in der Nacht zum Mittwoch alle wichtigen Betriebssysteme bis auf watchOS und HomePod OS aktualisiert. Es gibt Fixes und ein gestopftes Loch.

Updates für Mac und iPhone. (Bild: nikkimeel/Shutterstock.com)

12.03.2025, 07:30 Uhr Lesezeit: 2 Min. | Mac & i

KANN ICH AUCH SELBER BETROFFEN SEIN? OPFER WERDEN?

Patchday: Attacken auf Geräte mit Android 13, 14, 15 und 16 beobachtet

Google Android-Bugdroid vor Schloss-Symbol. (Bild: Primakov/Shutterstock.com)

02.12.2025, 10:59 Uhr Lesezeit: 2 Min. | Security

https://www.heise.de/news/Patchday-Attacken-auf-Geraete-mit-Android-13-14-15-und-16-beobachtet-11099576.html

KANN ICH AUCH SELBER BETROFFEN SEIN? OPFER WERDEN?

Mit wichtigem Sicherheitsupdate: macOS 15.3.2 und iOS 18.3.2 verfügbar

Apple hat in der Nacht zum Mittwoch alle wichtigen Betriebssysteme bis auf watchOS und HomePod OS aktualisiert. Es gibt Fixes und ein gestopftes Loch.

Updates für Mac und iPhone. (Bild: nikkimeel/Shutterstock.com)

12.03.2025, 07:30 Uhr Lesezeit: 2 Min. | Mac & i

https://www.heise.de/news/Mit-wichtigem-Sicherheitsupdate-macOS-15-3-2-und-iOS-18-3-2-verfuegbar-10312643.html

WAS KANN ICH MACHEN?

07

DIE „HAUSMITTEL“

- Virenschutz
  - und anlassbezogen sofortigen Fullscan, mindestens aber gelegentlich
- Patchen
  - muss wirklich alles installiert sein?
- Nicht auf alles klicken
  - Muss man wirklich auf alles klicken?
  - und wenn geklickt → Fullscan / PW wechseln
- Passwörter
  - Pro Account ein Passwort
  - Bei Verdacht auf Kompromittierung → PW wechseln

ES GIBT VIELE INFORMATIONSMÖGLICHKEITEN

ZWEI BEISPIELE

Bundesamt
für Sicherheit in der
Informationstechnik

https://www.bsi.bund.de/dok/6722626
https://www.bsi.bund.de/dok/CSN

Hamburg

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT

UND BLEIBEN SIE SICHER

Mediaserver Hamburg / Andreas Vallbracht

LSBG
Landesbetrieb Straßen,
Brücken und Gewässer
Hamburg

Hamburg