

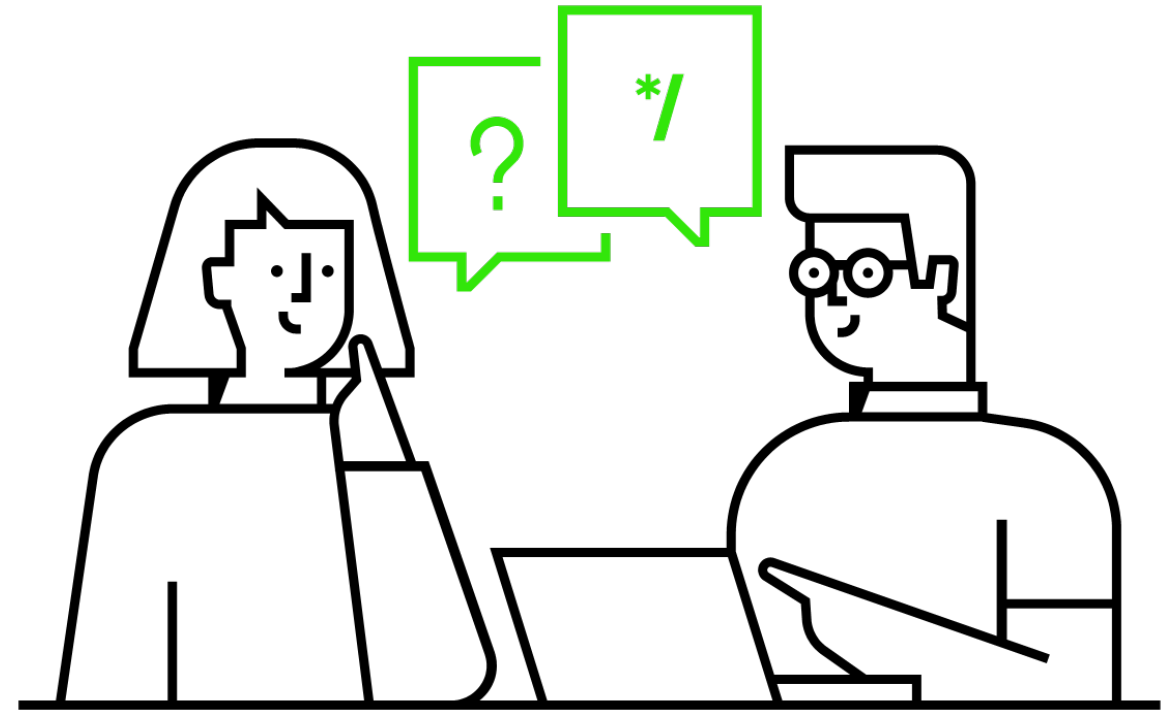
Quo vadis Rechenzentrum - Sicherheitsvorfall: was tun?

19. Kommunales IuK-Forum

Fachforum B1

Vortragender: Leif Erichsen - hannIT

08.09.2022



Agenda

- **Persönliche Vorstellung**
- **Sicherheitsvorfall**
- **sicheres RZ**
- **Handlungsempfehlung**
- **Nachbehandlung**
- **Weiterführende Informationen**

Persönliche Vorstellung

- **Leif Erichsen**
- **bei hannIT AöR seit 2013 (Team 3 - EWO, Team 1 - Kundenberatung, GB2-09 – KC Datenschutz & Informationssicherheit)**
- **seit 2018 externer Datenschutzbeauftragter für 18 Kommunen**
- **seit 04/2022**
 - externer Datenschutzbeauftragter für weitere 12 Kommunen
 - interner Datenschutzbeauftragter für hannIT AöR
 - KCM Datenschutz & Informationssicherheit
- **Referent (EuroAcad, Leibniz Universität Hannover, Hochschule Hannover, diverse kommunale Foren)**

Sicherheitsvorfall: Was heißt das?

Ein Sicherheitsvorfall ist immer eine Einschränkung der Schutzziele



Ein **Sicherheitsvorfall** ist nicht für jede Institution gleich, sondern muss immer **geeignet definiert** werden. Eine Abgrenzung zu einer Störung ist notwendig. Dazu müssen der Schutzbedarf der Daten, Auswirkungen auf die Aufgabenerfüllung, Finanzielle Auswirkungen, etc. betrachtet werden.

Die letztendliche **Definition** eines Sicherheitsvorfalls sollte **dokumentiert** und für alle sichtbar sein, deshalb sollte diese in der Leitlinie oder einem Prozess aufgeschrieben sein.

Sicherheitsvorfall: Was heißt das?

Gefährdungen:

- **Naturereignisse / Umwelteinflüsse**
- **Ausfall und Störungen**
- **Spionage**
- **Diebstahl und Verlust**
- **Fehlplanungen / Fehlfunktion / menschliches Versagen**
- **Schwachstellen**
- **Schadprogramme / DDoS / Social Engineering**
- **...**

Auswirkungen:

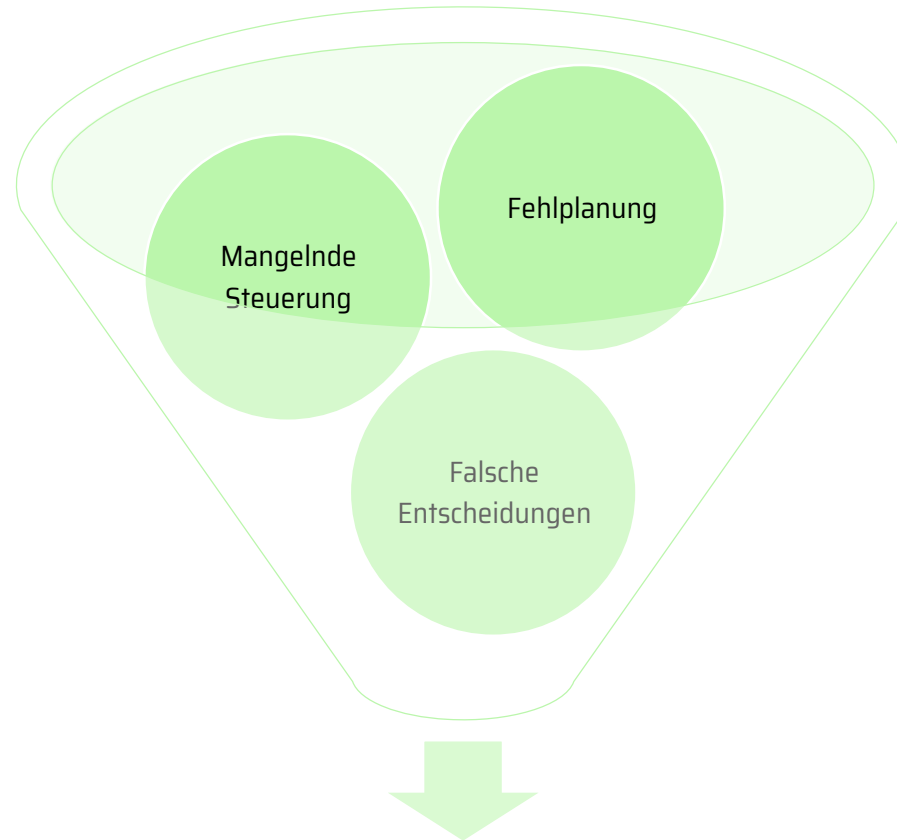
- **Einschränkung der Aufgabenerfüllung**
- **Zusätzliche (hohe) Kosten**
- **In der Regel reputationsschädigend**
- **Offenlegung von Informationen**
- **Ausfall existenzieller IT-Dienste**
- **Datenverlust**
- **...**

Risiken bei der Behandlung

Durch ungeplante Behandlung wird aus einem Sicherheitsvorfall schnell ein größeres Sicherheitsproblem.

Lösung:

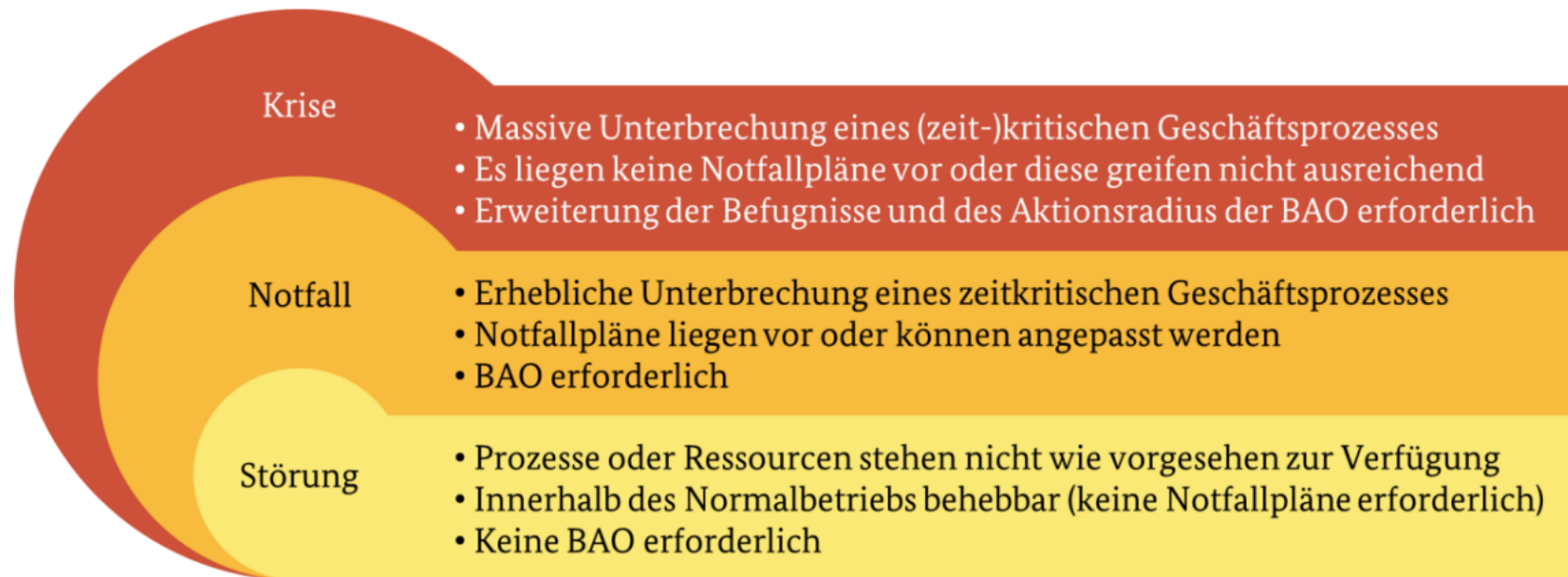
- Planung von Abläufen/Prozessen
- Festlegung von Verantwortlichkeiten
- Schaffung von Kompetenzen



Größere Schäden mit möglichen katastrophalen Folgen

Was ist ein Notfall?

Notfälle sind Unterbrechungen des Geschäftsbetriebs, die mindestens einen zeitkritischen Geschäftsprozess betreffen, der nicht im Normalbetrieb innerhalb der maximal tolerierbaren Ausfallzeit wiederhergestellt werden kann. (vgl. 2021, BSI-Standard 200-4)

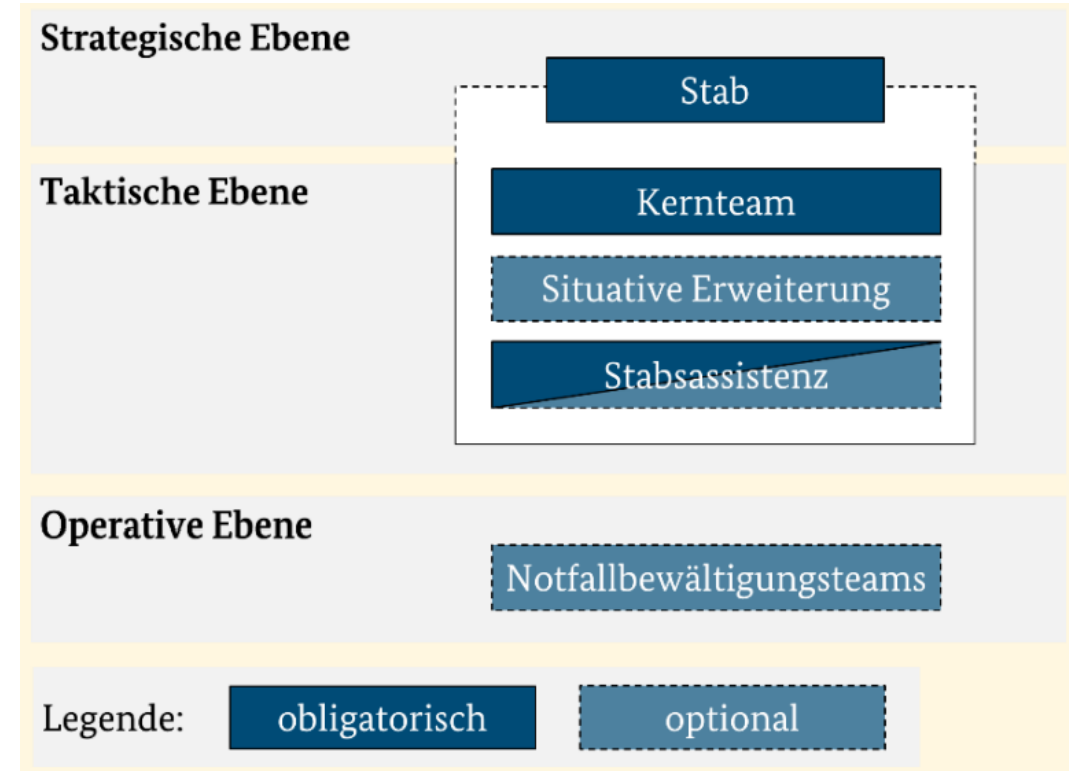


Abgrenzung Störung, Notfall, Krise (BAO = Besondere Aufbauorganisation), BSI-Standard 200-4

Notfallbehandlung

Erfordert speziellen Prozess (Notfallbehandlung)
Erfordert BAO (Besondere Aufbauorganisation)
Erfordert Wiederanlaufpläne/Notfallpläne

Eine Besondere Aufbauorganisation sorgt für eine zielgerichtete und rasche Bewältigung der Notfall- bzw. Krisensituation. Die BAO erhält hierfür bestimmte Entscheidungs- und Handlungsvollmachten von der Institutionsleitung.



Beispiel einer BAO (BSI-Standard 200-4)

Sicherheitsvorfall / Notfall - Beispiele

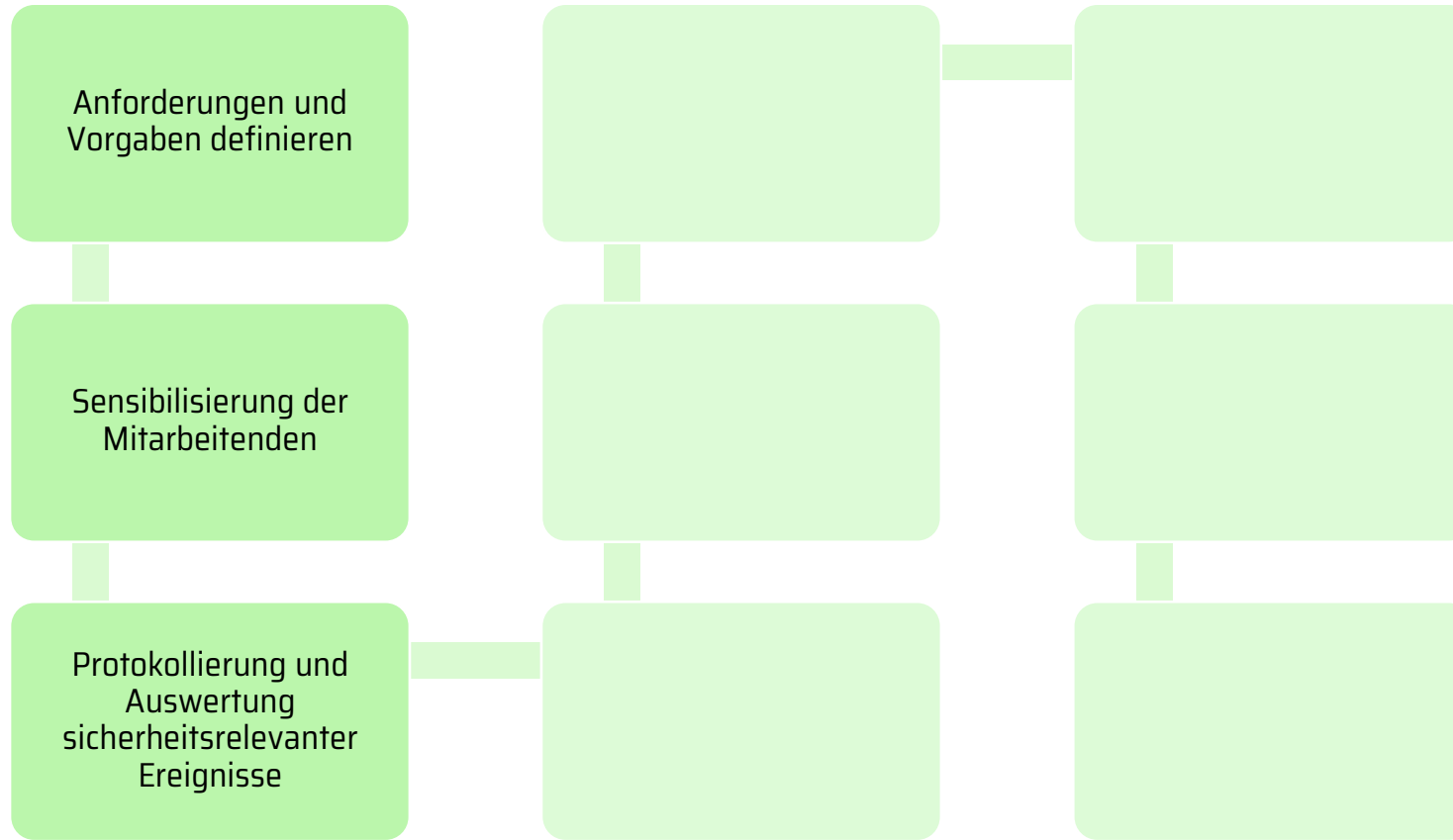
[BSI - 1.5 Definitionen \(bund.de\)](https://www.bund.de/portal/bsi/1.5-Definitionen)

Erst dann, wenn Störungen oder Ausfälle größere Schäden verursachen können und ihre Behebung mit den üblichen Verfahren nicht mehr möglich ist, erfordern sie ein Notfallmanagement. Beispiele:

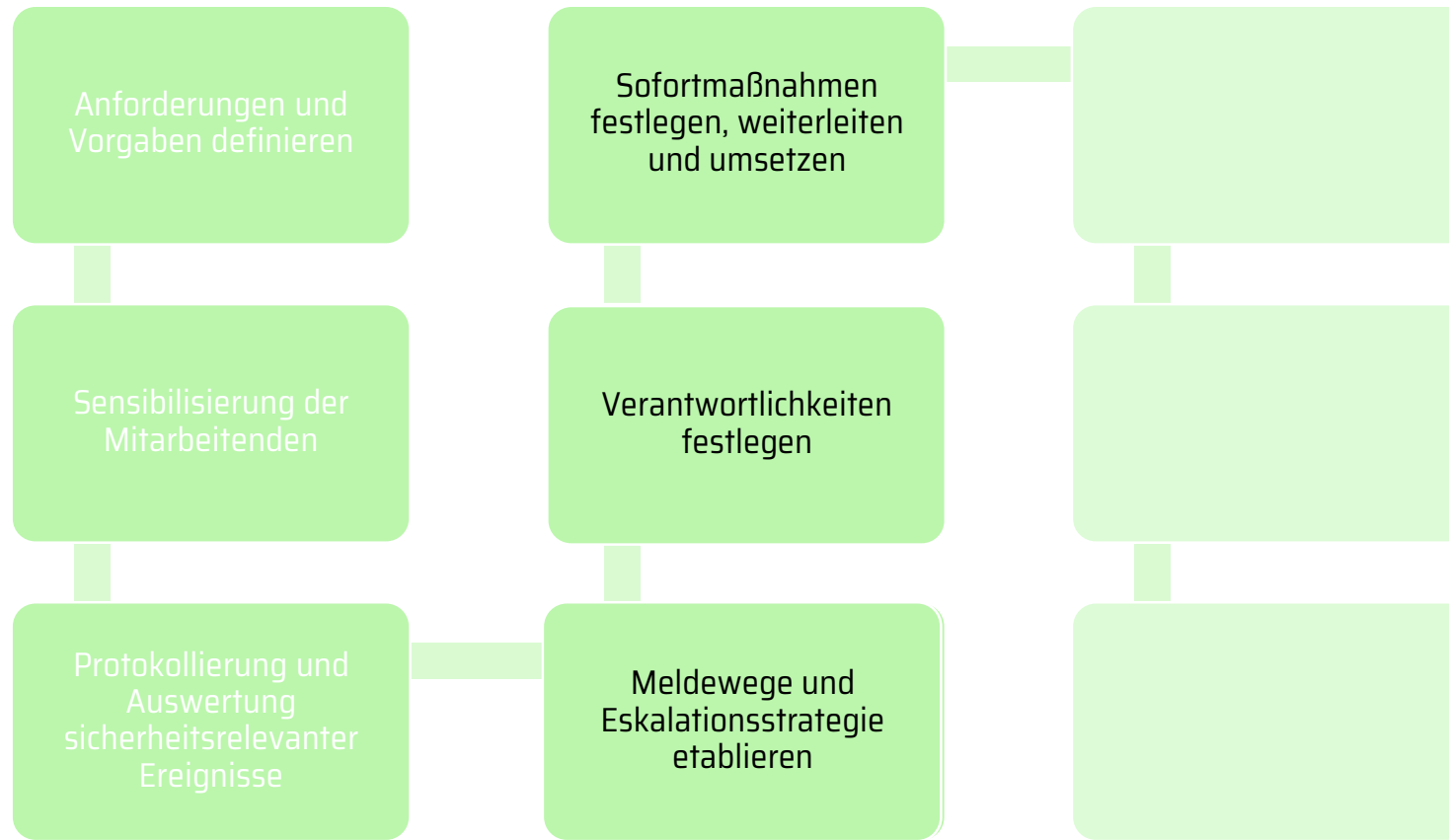
- Durch Brände können wichtige Betriebsräume (z. B. das Rechenzentrum oder eine Fertigungshalle) nicht mehr genutzt werden.
- Überschwemmungen führen zur tagelangen Sperrung von Zufahrtswegen.
- Eine Pandemie führt zu erheblichem Personalausfall.
- Das Stromnetz fällt flächendeckend und über einen längeren Zeitraum hinweg aus.
- Wichtige Kommunikationsnetze (Internet, Telefonnetz) fallen tagelang aus.
- Wichtige Lieferungen fallen vollständig aus, weil ein Lieferant Konkurs anmelden musste und auch nicht auf Ersatzlieferanten zurückgegriffen werden kann.

Ablauf Sicherheitsvorfall nach Phasen am Beispiel DDoS-Angriff

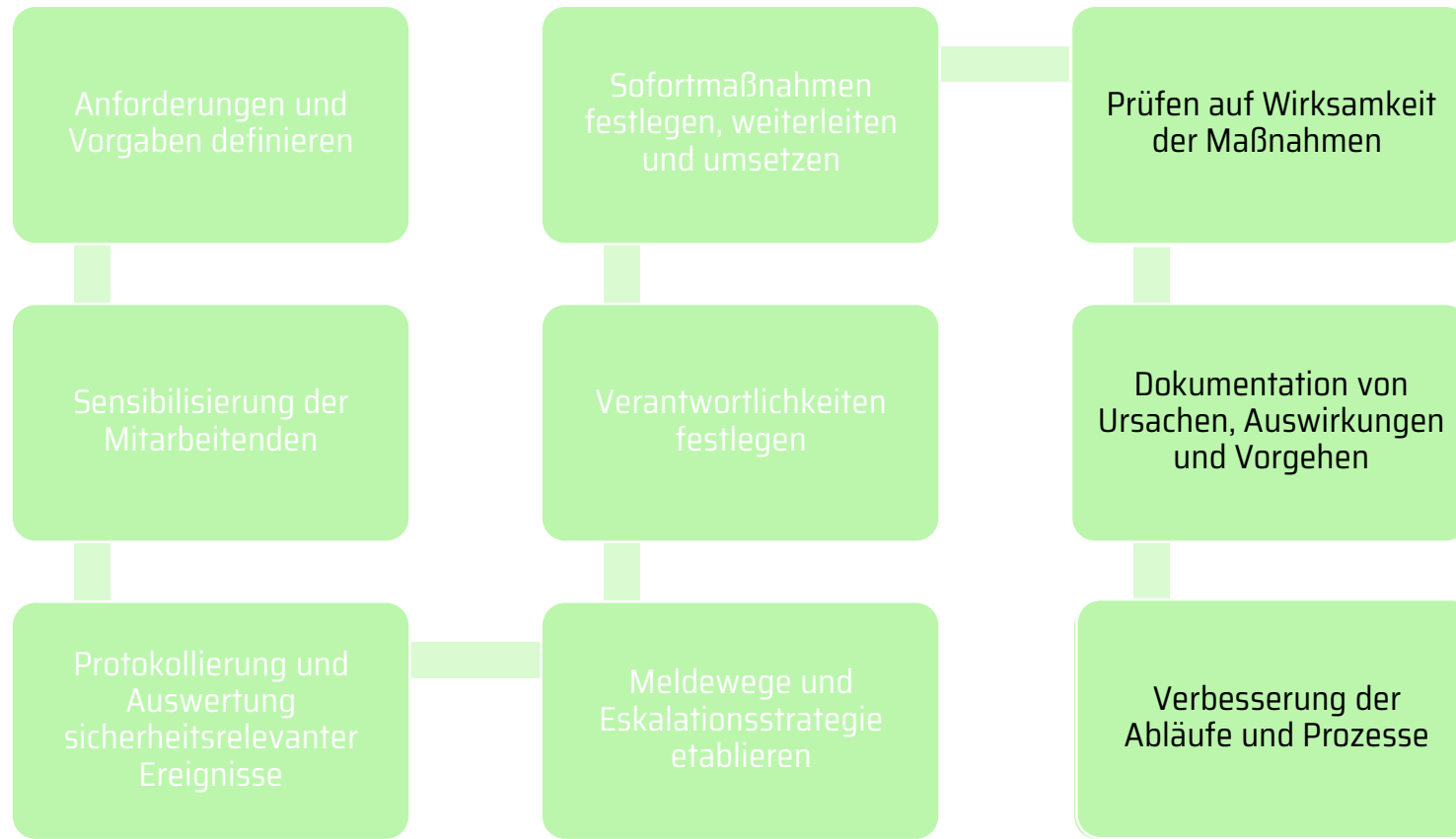
Detektion



Reaktion

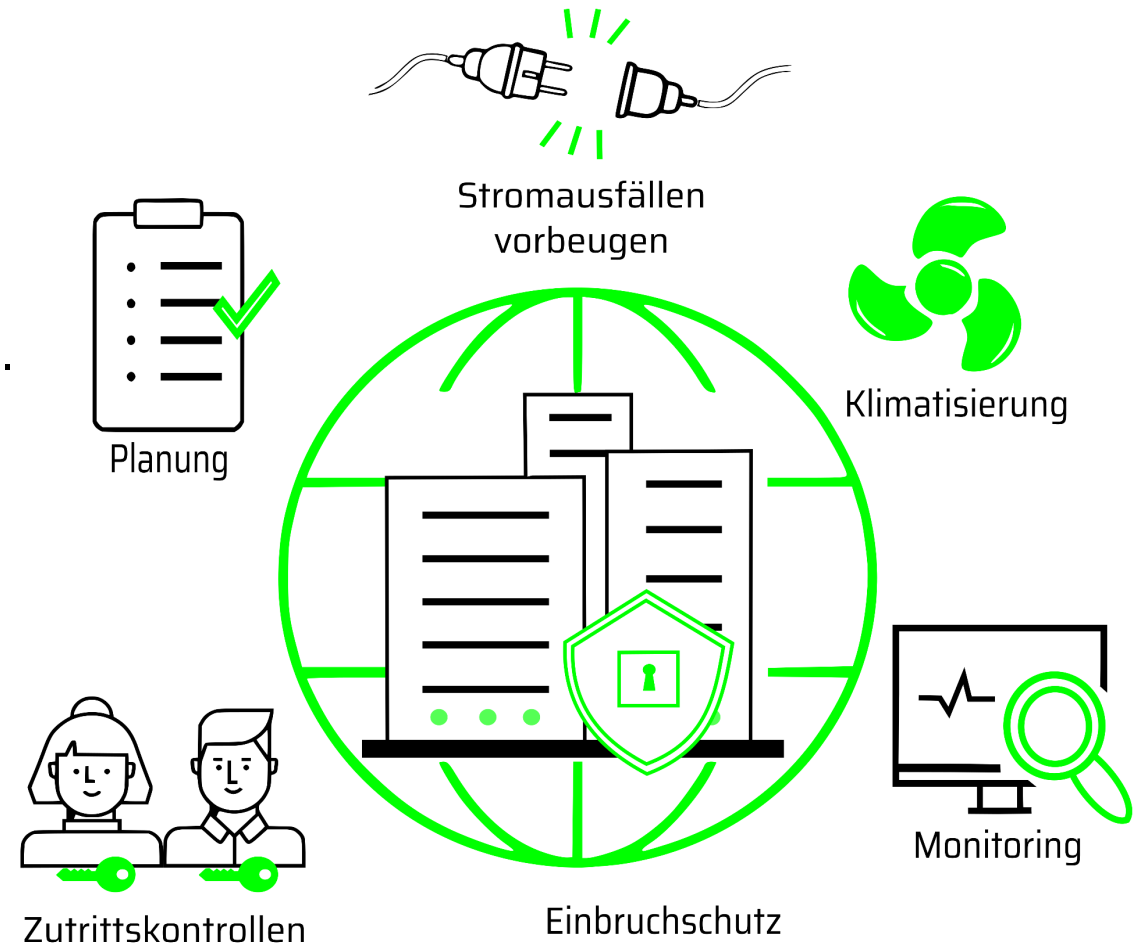


Nachbereitung




Was macht ein sicheres Rechenzentrum aus?

- **Richtige Planung**
 - * Absicherung gegen Gefährdungen durch elementare Gegebenheiten z.B.
 - * Überschwemmungen, Erdbeben, Brände etc.
 - * Flugverkehr
 - * genügend Bandbreite einplanen
- **Zutrittskontrollen**
- **Überwachung**
 - * Ausfälle müssen rechtzeitig bemerkt werden
- **Klimatisierung**
- **Einbruchschutz**
- **Absicherung gegen Stromausfälle**




Handlungsempfehlung und erste Schritte

- **Sicherheitsvorfall und Notfall definieren**
- **Sicherheitsrelevante Ereignisse definieren und überwachen / aktive Protokollierung**
- **Kommunikation: Melde- und Eskalationswege etablieren**
- **Notfallpläne erstellen**
 - Notfallkommunikation, Notfallhandbuch
- **Mitarbeitende sensibilisieren**
- **Üben und testen der Abläufe und Kommunikationswege**




VERHALTEN BEI IT-NOTFÄLLEN 

 **Ruhe bewahren & IT-Notfall melden**
Lieber einmal mehr als einmal zu wenig anrufen!


 IT-Notfallrufnummer:

 Wer meldet?

 Welches IT-System ist betroffen?

 Wie haben Sie mit dem IT-System gearbeitet?
Was haben Sie beobachtet?

 Wann ist das Ereignis eingetreten?

 Wo befindet sich das betroffene IT-System?
(Gebäude, Raum, Arbeitsplatz)

Verhaltenshinweise

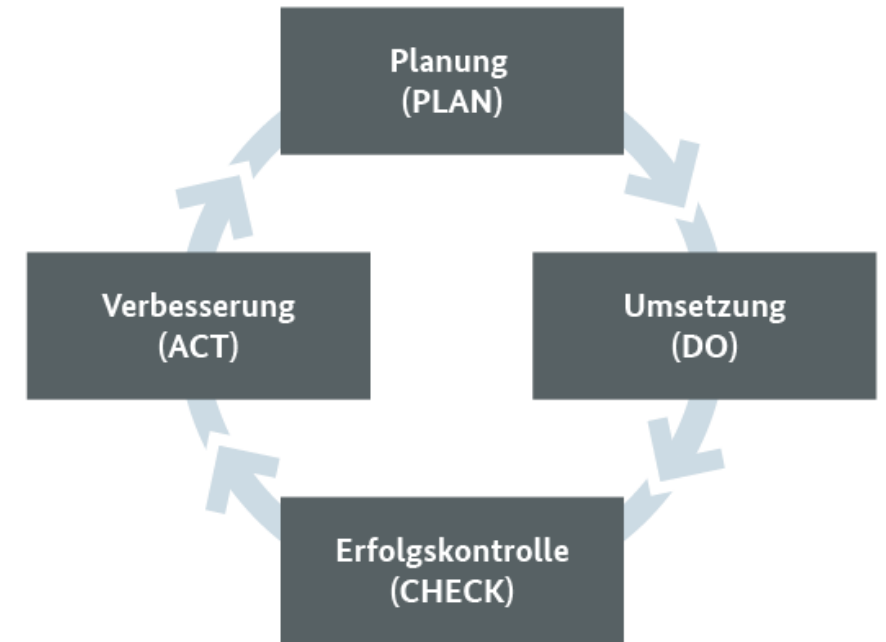
Weitere Arbeit am IT-System einstellen	Beobachtungen dokumentieren	Maßnahmen nur nach Anweisung einleiten
--	-----------------------------	--

Herausgeber: Bundesamt für Sicherheit in der Informationstechnik

[ACS - Allianz für Cyber-Sicherheit - ACS - IT-Notfallkarte "Verhalten bei IT-Notfällen", DIN A4, Raum für eigenes Logo \(allianz-fuer-cybersicherheit.de\)](https://www.allianz-fuer-cybersicherheit.de)

Nachbehandlung / Lessons Learned

- **Sicherheitsvorfallsbericht ausfüllen**
- **Was kann man aus dem Sicherheitsvorfall lernen?**
 - Müssen Ergänzungen bei den Dokumentationen vorgenommen werden?
 - Muss der Prozess angepasst werden?
 - Traten Probleme auf, wie können diese behoben werden?
 - Müssen Einstellungen angepasst werden?
 - Werden zusätzliche Dienstleister benötigt?
 - Wurde ausreichend kommuniziert?
 - Zuständigkeiten/ Rollen unklar?
 - ...
- **Änderungen in das ISMS einfließen lassen**



[BSI - Lerneinheit 2.1: Der Sicherheitsprozess \(bund.de\)](https://www.bund.de/Content/DE/BS/Lernen/2017/07/20170720-BSI-Lerneinheit-2-1-der-Sicherheitsprozess.html)

Was noch zu beachten wäre...

Ein Sicherheitsvorfall kann auch ein Datenschutzverstoß bedeuten, wenn personenbezogene Daten betroffen sind.

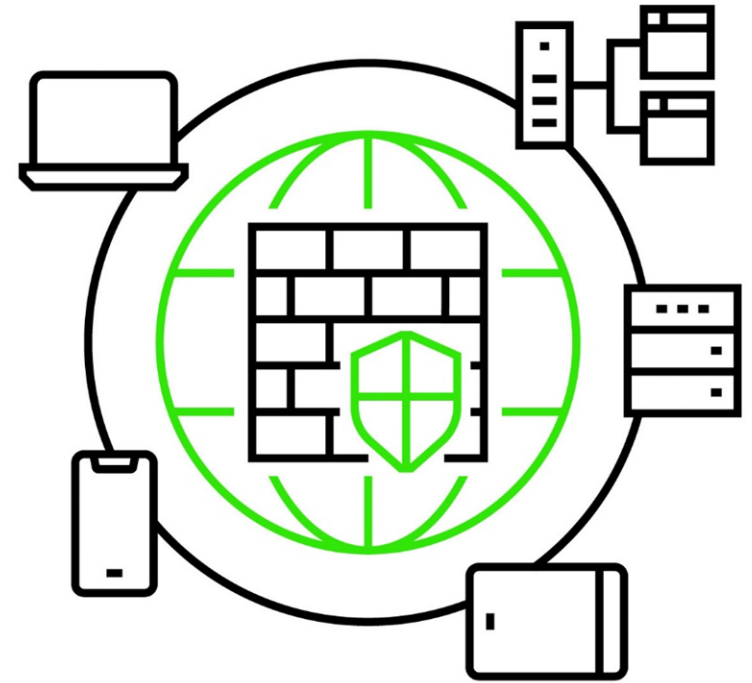
- **Art. 33 EU-DSGVO findet Anwendung**
 - Einbeziehung weiterer Gremien / Mitwirkende, wie z.B. Datenschutzbeauftragter, Informationssicherheitsbeauftragter, FD-Leitungen, N-CERT, etc.
 - Bewertung meldepflichtiger / nicht-meldepflichtiger Vorfall
 - Meldefrist 72 Std. ab Bekanntwerden durch den Verantwortlichen
 - Prüfung, ob die betroffene Personen über den Datenschutzverstoß informiert werden müssten (vgl. Art. 34 EU-DSGVO)
 - schriftliche Dokumentation
- **TOMs anpassen / „aktueller Stand der Technik“ → lessons learned (vgl. vorherige Folie)**

Weiterführende Informationen

BSI Standards

Bausteine aus dem BSI Grundschutz Kompendium 2022

- **DER.1** Detektion von sicherheitsrelevanten Ereignissen
- **DER.2.1** Behandlung von Sicherheitsvorfällen
- **DER.2.3** Bereinigung weitreichender Sicherheitsvorfälle
- **OPS.2.1** Outsourcing für Kunden
- **INF.2** Rechenzentrum sowie Serverraum





Hannoversche
Informationstechnologien AöR
Kompetenzcenter Informationssicherheit und Datenschutz
Hildesheimer Str. 47
30169 Hannover



0511 700 40 - 100
informationssicherheit@hannit.de



hannIT.de