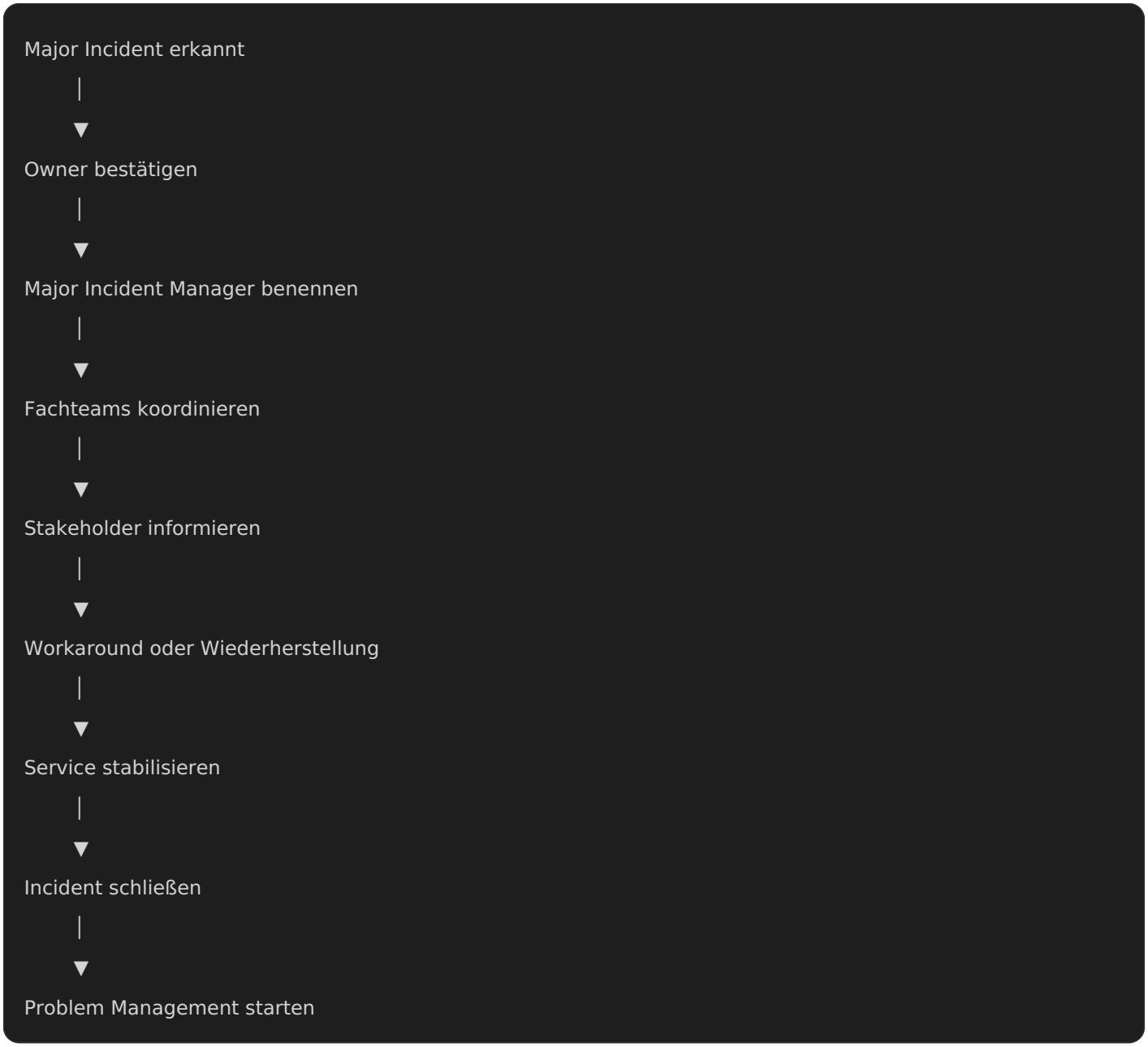
3.7 Ownership, hierarchische Eskalation und Major Incidents (Teil 2/2)

Major-Incident-Prozess

Nach der Einstufung als Major Incident beginnt eine koordinierte Bearbeitung.

Ein möglicher Ablauf:



Nicht jede Organisation verwendet exakt diesen Ablauf. Entscheidend ist eine klare Koordination.

War Room

Bei kritischen Incidents wird häufig ein gemeinsamer Kommunikationskanal eingerichtet.

Beispiele:

- Microsoft Teams
- Slack
- Telefonkonferenz
- Videokonferenz

Alle beteiligten Teams arbeiten dort gemeinsam.

Vorteile:

- schnellere Entscheidungen
- weniger Rückfragen
- keine Informationsverluste
- bessere Zusammenarbeit

Kommunikationsregeln

Während eines Major Incidents sollte Kommunikation:

- regelmäßig erfolgen,
- sachlich bleiben,
- bestätigte Fakten enthalten,
- Vermutungen klar kennzeichnen,
- Verantwortlichkeiten nennen,
- nächste Schritte erläutern.

Ungeeignet:

> Wir glauben, dass wahrscheinlich vielleicht die Firewall schuld ist.

Besser:

> Die Ursache wird aktuell untersucht. Firewall und Netzwerk werden geprüft. Nächste Statusmeldung um 11:30 Uhr.

Stakeholder

Nicht jeder benötigt dieselben Informationen.

Stakeholder	Benötigte Informationen
Benutzer	Auswirkungen und Workaround
Service Desk	aktueller Status
Management	Geschäftsrisiken
Kunden	Serviceverfügbarkeit
Technik	Diagnoseinformationen
Lieferanten	technische Details

Informationen sollten zielgruppengerecht formuliert werden.

Single Point of Communication

Bei großen Incidents sollte möglichst nur eine abgestimmte Kommunikationsquelle verwendet werden.

Dadurch werden widersprüchliche Aussagen vermieden.

Beispiele:

- Statusseite
- Incident Manager
- Kommunikationsverantwortlicher

Ressourcen koordinieren

Nicht jedes Team sollte unabhängig arbeiten.

Der Major Incident Manager achtet darauf, dass:

- Aufgaben verteilt,
- Doppelarbeiten vermieden,
- Ergebnisse zusammengeführt,
- Abhängigkeiten erkannt,
- und nächste Schritte eindeutig zugewiesen werden.

Dokumentation

Auch unter Zeitdruck muss dokumentiert werden.

Mindestens festhalten:

- Zeitpunkt

- Maßnahme
- Ergebnis
- Entscheidung
- Verantwortlicher

Diese Informationen werden später benötigt für:

- Problem Management
- Lessons Learned
- Audits
- Verbesserungen

Nach der Wiederherstellung

Mit der Wiederherstellung endet der Major Incident nicht vollständig.

Es folgen häufig:

- Ursachenanalyse
- Review
- Verbesserung
- Knowledge-Artikel
- Monitoring-Anpassungen
- Automatisierungen

Major Incident Review

Nach Abschluss sollte überprüft werden:

- Was ist passiert?
- Warum?
- Welche Maßnahmen waren erfolgreich?
- Wo gab es Verzögerungen?
- Welche Verbesserungen sind möglich?

Ziel ist Lernen – nicht Schuldzuweisung.

Lessons Learned

Typische Ergebnisse:

- bessere Dokumentation
- neue Checklisten
- Monitoring erweitern
- Alarmgrenzen anpassen

- Runbooks verbessern
- Schulungen durchführen
- Automatisierungen ergänzen

Problem Management einbeziehen

Ein Major Incident endet häufig mit einem neuen Problem Record.

Dadurch kann später untersucht werden:

- eigentliche Ursache
- dauerhafte Lösung
- Vermeidung zukünftiger Incidents

Häufige Fehler

Fehler 1

Kein eindeutiger Owner.

Fehler 2

Mehrere Teams arbeiten ohne Koordination.

Fehler 3

Benutzer erhalten keine Statusinformationen.

Fehler 4

Zu späte Eskalation.

Fehler 5

Jeder kommuniziert etwas anderes.

Fehler 6

Techniker diskutieren Vermutungen als Fakten.

Fehler 7

Keine Dokumentation während des Incidents.

Fehler 8

Nach Wiederherstellung erfolgt keine Nachbereitung.

Fehler 9

Lessons Learned werden nicht umgesetzt.

Fehler 10

Problem Management wird nicht gestartet.

Praxisbeispiel

08:15 Uhr

Mehrere Standorte melden Ausfälle.

08:20 Uhr

Major Incident aktiviert.

08:25 Uhr

Incident Manager übernimmt Koordination.

08:30 Uhr

Statusmeldung veröffentlicht.

08:40 Uhr

Netzwerk-, Server- und Cloud-Team arbeiten gemeinsam.

09:05 Uhr

Workaround verfügbar.

09:40 Uhr

Service vollständig wiederhergestellt.

10:30 Uhr

Review-Termin geplant.

Checkliste Ownership

- [ ] Owner eindeutig festgelegt
- [ ] Verantwortlichkeiten bekannt
- [ ] Benutzer informiert
- [ ] Eskalationen überwacht
- [ ] Ticket aktiv verfolgt

Checkliste Eskalation

- [ ] richtige Eskalationsart gewählt
- [ ] Fachinformationen vollständig
- [ ] richtige Ansprechpartner beteiligt
- [ ] Entscheidungen dokumentiert
- [ ] Status kommuniziert

Checkliste Major Incident

- [ ] Major Incident bestätigt
- [ ] Incident Manager benannt
- [ ] Kommunikationskanal eingerichtet
- [ ] Stakeholder informiert
- [ ] Workaround geprüft
- [ ] Maßnahmen dokumentiert
- [ ] regelmäßige Statusmeldungen
- [ ] Wiederherstellung bestätigt
- [ ] Review geplant
- [ ] Problem Record erstellt, falls erforderlich

Bedeutung für Fachinformatiker für Systemintegration

Auch wenn Fachinformatiker nicht die Rolle des Incident Managers übernehmen, sind sie häufig maßgeblich an der technischen Analyse beteiligt.

Im Arbeitsalltag bedeutet das:

- strukturiert arbeiten,
- Ergebnisse dokumentieren,
- Änderungen nachvollziehbar durchführen,
- sauber kommunizieren,
- und andere Teams aktiv unterstützen.

Gerade bei größeren Störungen entscheidet oft die Zusammenarbeit über die Dauer des Ausfalls.

Zusammenfassung

> Incident übernehmen
> ↓
> Owner festlegen
> ↓
> Bearbeitung koordinieren
> ↓
> falls notwendig funktional oder hierarchisch eskalieren
> ↓
> Major Incident aktivieren, wenn Kriterien erfüllt
> ↓
> Kommunikation sicherstellen
> ↓
> Service wiederherstellen
> ↓
> Review durchführen
> ↓
> Erkenntnisse in Problem Management und Continual Improvement übernehmen

---

Verwandte Seiten

- 3.5 Auswirkungen, Dringlichkeit und Priorität
- 3.6 Erstdiagnose, Lösung und funktionale Eskalation
- 3.8 Self-Service, Wissensnutzung und Automatisierung
- Problem Management
- Knowledge Management
- Continual Improvement

Quellen

- PeopleCert – ITIL 4 / ITIL 5 Incident Management
- PeopleCert – ITIL 4 / ITIL 5 Service Desk
- PeopleCert – ITIL Practice Guides

- ITIL Service Version 5

Framework-Stand: ITIL Version 5
Fachlicher Stand: August 2026
