3.6 Erstdiagnose, Lösung und funktionale Eskalation (Teil 1/2)

> **Kurz erklärt**
>
> Ziel der Erstdiagnose ist nicht, sofort die eigentliche Ursache zu kennen, sondern möglichst schnell die Situation zu verstehen, Auswirkungen zu begrenzen und den Service wiederherzustellen.
>
> Gute Diagnosen beruhen auf:
>
> - Beobachtungen,
> - überprüfbaren Fakten,
> - strukturierten Tests,
> - technischem Wissen,
> - vorhandenen Erfahrungen,
> - und nachvollziehbaren Entscheidungen.
>
> ITIL empfiehlt, vorhandenes Wissen systematisch zu nutzen und Incidents möglichst früh dort zu lösen, wo die erforderlichen Fähigkeiten vorhanden sind.

Ziele der Erstdiagnose

Nach der Ticketaufnahme beginnt die eigentliche Analyse.

Dabei sollten zunächst folgende Fragen beantwortet werden:

- Was funktioniert nicht?
- Was funktioniert noch?
- Seit wann besteht die Störung?
- Wer ist betroffen?
- Welche Änderungen gab es kurz zuvor?
- Welche Systeme hängen zusammen?
- Gibt es bereits bekannte Incidents?
- Existiert ein Workaround?

Die Erstdiagnose soll möglichst schnell klären,

- ob der Service wiederhergestellt werden kann,

- ob Spezialisten benötigt werden,
- oder ob eine funktionale Eskalation notwendig ist.

Erstdiagnose ist keine Ursachenanalyse

Ein häufiger Fehler besteht darin, bereits in den ersten Minuten die eigentliche Ursache finden zu wollen.

Die Erstdiagnose verfolgt jedoch ein anderes Ziel.

Erstdiagnose	Ursachenanalyse
Service möglichst schnell wiederherstellen	eigentliche Ursache dauerhaft finden
Minuten bis Stunden	Stunden bis Tage
Incident Management	Problem Management
Fokus auf Wiederherstellung	Fokus auf Prävention

Beispiel:

Ein Webserver antwortet nicht.

Während der Erstdiagnose genügt möglicherweise:

- Dienst neu starten,
- Funktion prüfen,
- Benutzer informieren.

Warum der Dienst abgestürzt ist, wird später im Problem Management untersucht.

> **Merke**
>
> Ein gelöster Incident bedeutet nicht automatisch, dass die Ursache beseitigt wurde.

Beobachtung vor Interpretation

Techniker neigen häufig dazu, sehr früh Vermutungen aufzustellen.

Besser ist folgende Reihenfolge:

1. Beobachten
2. Informationen sammeln
3. Hypothesen bilden
4. Hypothesen testen
5. Ursache bestätigen

Beispiel:

 "Die Firewall blockiert den Zugriff."

Besser:

 "HTTPS-Verbindungen schlagen fehl. Andere Protokolle funktionieren. Firewall ist eine mögliche Ursache."

Symptome richtig erfassen

Ein Symptom beschreibt das beobachtete Verhalten.

Beispiele:

- Anmeldung schlägt fehl
- Druckauftrag bleibt hängen
- Anwendung reagiert nicht
- Datei lässt sich nicht öffnen
- VPN verbindet nicht

Ein Symptom ist noch keine Ursache.

Mögliche Ursachen

Für dasselbe Symptom können völlig unterschiedliche Ursachen verantwortlich sein.

Symptom

> Anmeldung nicht möglich

Mögliche Ursachen:

- Passwort falsch
- Konto gesperrt
- Active Directory nicht erreichbar
- DNS-Problem
- Netzwerkfehler
- Zertifikat abgelaufen
- MFA-Dienst gestört
- Cloud-Ausfall

Deshalb sollten Vermutungen immer überprüft werden.

Strukturierte Diagnose

Eine bewährte Reihenfolge lautet:

1. Problem verstehen
2. Umfang bestimmen
3. Änderungen prüfen
4. Logs prüfen
5. Monitoring prüfen
6. Verbindung testen
7. Komponenten eingrenzen
8. Hypothese testen
9. Ergebnis dokumentieren

Umfang bestimmen

Nicht jede Störung betrifft alle Benutzer.

Zu klären ist:

- Ein Benutzer?
- Mehrere Benutzer?
- Ein Standort?
- Alle Standorte?
- Nur Windows?
- Auch macOS?
- Nur VPN?
- Auch intern?

Je genauer der Umfang bekannt ist, desto einfacher lässt sich die Ursache eingrenzen.

Änderungen berücksichtigen

Viele Incidents entstehen kurz nach Änderungen.

Zu prüfen sind beispielsweise:

- Software-Updates
- neue Firewall-Regeln
- Zertifikatswechsel
- DNS-Änderungen
- neue Switch-Konfiguration
- Benutzeränderungen
- Gruppenrichtlinien
- Cloud-Änderungen

Frage:

> **Was hat sich kurz vor dem Fehler geändert?**

Diese Frage spart häufig sehr viel Diagnosezeit.

Reproduzierbarkeit prüfen

Ein Fehler sollte möglichst reproduziert werden.

Beispiel:

1. Anwendung starten
2. Benutzer anmelden
3. Auftrag öffnen
4. Speichern

Tritt der Fehler jedes Mal auf?

Oder nur gelegentlich?

Auch diese Information grenzt Ursachen erheblich ein.

Bekannte Fehler nutzen

Vor aufwendigen Analysen sollte geprüft werden:

- Gibt es einen bekannten Incident?
- Existiert ein Knowledge-Artikel?
- Hat der Hersteller bereits einen Hinweis veröffentlicht?
- Gab es ähnliche Tickets?

Viele Incidents lassen sich dadurch deutlich schneller lösen.

Monitoring verwenden

Monitoring liefert häufig frühere Hinweise als Benutzer.

Beispiele:

- CPU-Auslastung
- RAM
- Festplattenspeicher
- Netzwerk
- Dienste
- Zertifikate
- Backup
- Hardware

Monitoring ersetzt jedoch keine Diagnose.

Es zeigt häufig nur Symptome.

Logs richtig einsetzen

Logs beantworten häufig Fragen wie:

- Wann trat der Fehler auf?
- Welche Komponente war beteiligt?
- Welche Fehlermeldung wurde erzeugt?
- Welche Benutzer waren betroffen?

Dabei gilt:

Nicht jede Warnung ist automatisch relevant.

Logs müssen immer im Zusammenhang betrachtet werden.

Ausschlussverfahren

Eine sehr effektive Methode ist das Ausschlussprinzip.

Beispiel:

VPN funktioniert nicht.

Prüfung:

- Internet vorhanden ✔
- DNS funktioniert ✔
- Anmeldung funktioniert ✔
- VPN-Server erreichbar ✔
- Zertifikat gültig □

Die Ursache lässt sich dadurch systematisch eingrenzen.

Von einfach nach komplex

ITIL empfiehlt keine feste Reihenfolge.

In der Praxis hat sich jedoch bewährt:

1. Offensichtliches prüfen
2. Bekannte Fehler prüfen
3. Änderungen prüfen
4. Monitoring prüfen
5. Logs prüfen
6. Detailanalyse

Nicht sofort mit der kompliziertesten Hypothese beginnen.

Keine unnötigen Änderungen

Während der Diagnose sollte möglichst nicht gleichzeitig an mehreren Komponenten gearbeitet werden.

Schlecht:

- Firewall ändern
- DNS ändern
- Server neu starten
- Zertifikat erneuern

Danach ist kaum nachvollziehbar, welche Maßnahme tatsächlich geholfen hat.

Besser:

Eine Änderung durchführen.

Ergebnis prüfen.

Dokumentieren.

Erst danach die nächste Maßnahme.

Hypothesen dokumentieren

Eine gute Arbeitsnotiz enthält:

Hypothese

DNS-Auflösung fehlerhaft.

Test

Namensauflösung gegen internen DNS geprüft.

Ergebnis

DNS funktioniert.

Schlussfolgerung

Hypothese verworfen.

Dadurch vermeiden andere Bearbeiter dieselben Tests.

Wissen systematisch nutzen

Erfahrungen sollten nicht ausschließlich im Kopf einzelner Administratoren bleiben.

Hilfreich sind:

- Knowledge-Artikel
- Standardlösungen
- Runbooks
- Checklisten
- bekannte Fehler
- Herstellerdokumentation

Dadurch steigt die First Contact Resolution deutlich.

First Contact Resolution (FCR)

FCR beschreibt den Anteil der Incidents,

die bereits beim ersten Kontakt vollständig gelöst werden.

Vorteile:

- kürzere Wartezeit
- zufriedenere Benutzer

- weniger Eskalationen
- geringere Kosten

FCR darf jedoch nicht künstlich erhöht werden, indem Tickets vorschnell geschlossen werden.

Shift Left

Shift Left bedeutet,

Wissen möglichst früh im Support bereitzustellen.

Beispiele:

- bessere Wissensdatenbank
- Self-Service
- Standardlösungen
- Automatisierung
- KI-Unterstützung
- Schulungen

Dadurch können mehr Incidents bereits im Service Desk gelöst werden.

Dokumentation während der Diagnose

Nicht erst am Ende dokumentieren.

Nach jeder wichtigen Maßnahme sollte festgehalten werden:

- Zeitpunkt
- Maßnahme
- Ergebnis
- nächster Schritt

Dadurch bleiben Übergaben nachvollziehbar.

Merksätze

> Symptome sind keine Ursachen.

> Beobachtungen sind wichtiger als Vermutungen.

> Erst den Service wiederherstellen, anschließend die eigentliche Ursache untersuchen.

> Jede Diagnose sollte nachvollziehbar dokumentiert werden.

> Bekannte Lösungen sind schneller als neue Vermutungen.