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

> **Kurz erklärt**
>
> Die Erstdiagnose soll einen Incident schnell verstehen, eingrenzen und möglichst früh beheben.
>
> Dabei geht es zunächst nicht darum, die endgültige Ursache vollständig zu ermitteln. Das wichtigste Ziel des Incident Managements ist die schnelle Wiederherstellung des vereinbarten Servicebetriebs.
>
> Kann der Incident mit den vorhandenen Kenntnissen, Werkzeugen oder Berechtigungen nicht gelöst werden, erfolgt eine **funktionale Eskalation** an eine geeignete Fachgruppe.

Ziele der Erstdiagnose

Die Erstdiagnose soll möglichst schnell klären:

- Was funktioniert nicht?
- Was funktioniert weiterhin?
- Wer oder was ist betroffen?
- Seit wann besteht die Beeinträchtigung?
- Welche Auswirkungen entstehen?
- Gab es kurz zuvor einen Change?
- Ist bereits ein ähnlicher Incident bekannt?
- Existiert ein dokumentierter Workaround?
- Kann der Service Desk den Incident direkt lösen?
- Welche Fachkenntnisse werden andernfalls benötigt?

Eine gute Erstdiagnose reduziert:

- unnötige Rückfragen,
- doppelte Prüfungen,
- falsche Eskalationen,
- lange Bearbeitungszeiten,
- und vermeidbare Serviceunterbrechungen.

Erstdiagnose und Ursachenanalyse unterscheiden

Die Erstdiagnose gehört in erster Linie zum Incident Management.

Die tiefergehende Ursachenanalyse gehört häufig zum Problem Management.

Erstdiagnose	Ursachenanalyse
Service möglichst schnell wiederherstellen	zugrunde liegende Ursache untersuchen
kurzfristiger Fokus	langfristiger Fokus
Workaround oder schnelle Lösung möglich	dauerhafte Lösung vorbereiten
Incident Management	Problem Management
Minuten bis Stunden	abhängig von Komplexität auch deutlich länger

Beispiel:

Ein Anwendungsdienst reagiert nicht mehr.

Incident Management

- Dienst kontrolliert neu starten
- Funktion testen
- Benutzer informieren
- Service wiederherstellen

Problem Management

- Ursache des Absturzes untersuchen
- Speicherverbrauch analysieren
- Softwarefehler prüfen
- dauerhafte Korrektur planen

> **Merke**
>
> Ein Incident kann gelöst sein, obwohl die eigentliche Ursache noch nicht bekannt oder beseitigt ist.

Symptom, Ursache und Auswirkung unterscheiden

Begriff	Bedeutung	Beispiel
Symptom	beobachtetes Fehlverhalten	Anmeldung schlägt fehl
unmittelbare Ursache	direkter technischer Auslöser	Zertifikat abgelaufen
Grundursache	tiefer liegende Ursache	Zertifikatsüberwachung fehlte

Begriff	Bedeutung	Beispiel
Auswirkung	Folge für Benutzer oder Geschäftsprozess	Benutzer können nicht arbeiten

Zu Beginn eines Incidents ist häufig nur das Symptom bekannt.

Die Ursache darf deshalb nicht vorschnell als bestätigt dokumentiert werden.

Ungeeignet:

> Die Firewall blockiert die Anwendung.

Besser:

> HTTPS-Verbindungen zur Anwendung schlagen fehl. Eine Blockierung durch die Firewall ist eine mögliche, noch nicht bestätigte Ursache.

Beobachtung und Vermutung trennen

Eine strukturierte Diagnose folgt möglichst dieser Reihenfolge:

1. beobachten
2. Informationen sammeln
3. Umfang bestimmen
4. Hypothesen bilden
5. Hypothesen testen
6. Ergebnisse bewerten
7. Service wiederherstellen
8. Maßnahmen dokumentieren

Beobachtungen sollten möglichst messbar sein.

Ungeeignet:

> Das Netzwerk ist langsam.

Besser:

>

> Die Antwortzeit zum Gateway liegt normalerweise unter 5 ms. Aktuell werden zwischen 80 und 150 ms sowie Paketverluste von etwa 12 Prozent gemessen.

Den Umfang bestimmen

Der Umfang hilft bei der Eingrenzung.

Zu prüfen ist beispielsweise:

- Ist nur ein Benutzer betroffen?
- Sind mehrere Benutzer betroffen?
- Ist ein gesamter Standort betroffen?
- Betrifft der Fehler alle Geräte oder nur ein bestimmtes?
- Ist nur eine Anwendung betroffen?
- Funktioniert der Service intern, aber nicht über VPN?
- Sind nur neue Anmeldungen betroffen?
- Funktionieren bestehende Sitzungen weiterhin?
- Sind bestimmte Betriebssysteme oder Versionen betroffen?

Beispiel:

Eine Anwendung startet bei einem Benutzer nicht.

Prüfung:

- anderer Benutzer am selben Gerät: funktioniert
- derselbe Benutzer an anderem Gerät: funktioniert nicht
- andere Anwendungen: funktionieren

Damit liegt die Ursache wahrscheinlich eher im Benutzerkonto oder Benutzerprofil als im Gerät.

Den Normalzustand kennen

Für die Diagnose muss bekannt sein, was normalerweise geschehen sollte.

Beispiel:

> “ Nach Eingabe der Zugangsdaten sollte innerhalb weniger Sekunden die Startseite erscheinen. Stattdessen bleibt der Ladebildschirm dauerhaft sichtbar.

Diese Beschreibung ist aussagekräftiger als:

> Anmeldung funktioniert nicht.

Hilfreiche Fragen:

- Was wollten Sie durchführen?
- Was sollte normalerweise geschehen?
- Was geschieht stattdessen?
- Wird eine Fehlermeldung angezeigt?
- Wann hat es zuletzt funktioniert?

Änderungen berücksichtigen

Viele Incidents treten nach Änderungen auf.

Zu prüfen sind beispielsweise:

- Softwareupdates
- neue Firewall-Regeln
- DNS-Änderungen
- Zertifikatswechsel
- Gruppenrichtlinien
- Benutzer- oder Berechtigungsänderungen
- Firmwareupdates
- Netzwerkumbauten
- Cloud-Konfigurationsänderungen
- Änderungen durch Lieferanten

Eine wichtige Diagnosefrage lautet:

> “ Was hat sich kurz vor Beginn des Fehlers verändert?

Ein zeitlicher Zusammenhang beweist jedoch noch keine Ursache.

Der Change muss fachlich überprüft werden.

Bekannte Incidents und Fehler prüfen

Vor einer aufwendigen Analyse sollte geprüft werden:

- Gibt es bereits einen aktiven Incident?
- Ist eine allgemeine Störung bekannt?
- Existiert ein Problem Record?

- Gibt es einen Known Error?
- Ist ein geeigneter Knowledge-Artikel vorhanden?
- Hat der Hersteller eine Störung oder ein bekanntes Problem gemeldet?
- Wurde dieselbe Kombination aus Symptom und Service bereits dokumentiert?

Dadurch lassen sich doppelte Analysen vermeiden.

Monitoring verwenden

Monitoring kann wichtige Hinweise liefern.

Typische Messwerte:

- CPU-Auslastung
- Arbeitsspeicher
- Speicherplatz
- Dienststatus
- Netzwerkverbindungen
- Antwortzeiten
- Fehlerraten
- Zertifikatsgültigkeit
- Backup-Status
- Hardwarezustand
- Cloud-Service-Status

Monitoring zeigt jedoch häufig nur ein Symptom.

Beispiel:

> CPU-Auslastung 100 Prozent

Dies beweist noch nicht, welcher Prozess oder welche Ursache verantwortlich ist.

Logs gezielt auswerten

Logs können zeigen:

- wann ein Fehler begann,
- welche Komponente beteiligt war,
- welche Meldung erzeugt wurde,
- welches Konto verwendet wurde,
- und welche Aktion fehlgeschlagen ist.

Bei der Auswertung sollte geprüft werden:

- Passt der Zeitstempel zum Incident?
- Betrifft die Meldung wirklich den betroffenen Service?
- Ist es ein Fehler, eine Warnung oder nur eine Information?
- Tritt die Meldung auch im Normalbetrieb auf?
- Gibt es zeitlich passende Changes oder Events?

Nicht jede rote Fehlermeldung ist für den aktuellen Incident relevant.

Reproduzierbarkeit prüfen

Ein reproduzierbarer Fehler lässt sich leichter eingrenzen.

Zu dokumentieren sind:

- genaue Arbeitsschritte
- verwendete Anwendung
- Version
- Gerät oder Betriebssystem
- Benutzerkonto
- verwendete Daten
- erwartetes Verhalten
- tatsächliches Verhalten
- Fehlermeldung

Beispiel:

1. Anwendung öffnen
2. Auftrag auswählen
3. „PDF exportieren“ anklicken
4. Anwendung beendet sich ohne Meldung

Zusatz:

- tritt bei drei getesteten Aufträgen auf
- nur Desktop-Version betroffen
- Webversion funktioniert

Vom Einfachen zum Komplexen

Eine sinnvolle Praxisreihenfolge kann sein:

1. Meldung und Auswirkungen verstehen
2. bekannte Störungen prüfen

3. offensichtliche Voraussetzungen prüfen
4. Änderungen vergleichen
5. Monitoring und Logs auswerten
6. Fehlerbereich eingrenzen
7. Hypothesen testen
8. Spezialisten einbinden

Dies ist keine feste ITIL-Vorgabe.

Es verhindert jedoch, dass sofort mit besonders aufwendigen oder riskanten Maßnahmen begonnen wird.

Ausschlussverfahren

Beim Ausschlussverfahren werden mögliche Fehlerbereiche systematisch geprüft.

Beispiel:

VPN-Verbindung funktioniert nicht.

Prüfung	Ergebnis
Internetverbindung vorhanden	ja
DNS-Auflösung funktioniert	ja
VPN-Gateway erreichbar	ja
Benutzerkonto aktiv	ja
MFA erfolgreich	ja
Client-Zertifikat gültig	nein

Damit wurde der Fehler auf das Zertifikat eingegrenzt.

> **Merke**
>
> Jeder Test sollte eine konkrete Hypothese bestätigen oder verwerfen.

Hypothesen dokumentieren

Eine gute Arbeitsnotiz kann folgendermaßen aufgebaut sein:

Hypothese

DNS-Auflösung ist fehlerhaft.

Test

Interne und externe Namensauflösung mit dem vorgesehenen DNS-Server geprüft.

Ergebnis

Name wird korrekt aufgelöst.

Schlussfolgerung

Hypothese verworfen.

Dadurch muss die nächste bearbeitende Person denselben Test nicht wiederholen.

Nur kontrollierte Maßnahmen durchführen

Während der Diagnose sollten nicht mehrere Änderungen gleichzeitig vorgenommen werden.

Ungeeignet:

- DNS ändern
- Firewall-Regel anpassen
- Dienst neu starten
- Zertifikat erneuern
- Server neu starten

Wenn der Service anschließend funktioniert, ist nicht erkennbar, welche Maßnahme wirksam war.

Besser:

1. Maßnahme planen
2. Risiko bewerten
3. Maßnahme durchführen
4. Ergebnis prüfen
5. dokumentieren
6. erst danach nächsten Schritt festlegen

Produktive Änderungen müssen entsprechend den Regeln des Change Enablement durchgeführt werden.

Neustarts bewusst einsetzen

Ein Neustart kann ein sinnvoller Workaround sein.

Er darf jedoch nicht reflexartig verwendet werden.

Vorher sollte geprüft werden:

- Gehen flüchtige Diagnoseinformationen verloren?
- Werden Benutzer oder andere Services unterbrochen?
- Besteht Datenverlustrisiko?
- Ist eine Genehmigung erforderlich?
- Gibt es eine weniger eingreifende Maßnahme?
- Kann der Fehler nach dem Neustart weiterhin analysiert werden?

... *(Fortsetzung wegen Nachrichtenlängenlimit erforderlich)*