1.1 Störung strukturiert aufnehmen

Zweck dieser Seite

Diese Seite dient der vollständigen und einheitlichen Aufnahme einer IT-Störung.

Bevor mit der technischen Diagnose begonnen wird, müssen das sichtbare Problem, der Zeitpunkt, die betroffenen Systeme und die verfügbaren Beweise dokumentiert werden.

Eine gute Störungsaufnahme verhindert:

- falsche Annahmen;
- unnötige Tests;
- wiederholte Rückfragen;
- Verlust flüchtiger Informationen;
- Veränderungen ohne dokumentierten Ausgangszustand;
- unvollständige Eskalationen an andere Administratoren oder Hersteller.

Grundregel

Die Störung wird zunächst beschrieben, aber noch nicht bewertet.

Beispiel:

Nicht ausreichend:

> Das Netzwerk funktioniert nicht.

Besser:

> Der Client erhält seit dem 30.07.2026 um 14:35 Uhr über Ethernet keine DHCP-Adresse. Windows verwendet stattdessen die IPv4-Adresse 169.254.18.24. Über WLAN erhält derselbe Client eine gültige Adresse und kann auf interne Dienste zugreifen.

Die zweite Beschreibung enthält ein beobachtbares Symptom, einen Zeitpunkt, ein betroffenes Interface und einen funktionierenden Vergleich.

Die wichtigsten Informationen

Information	Fragestellung
Melder	Wer hat die Störung gemeldet?
Zeitpunkt	Wann wurde die Störung erstmals festgestellt?
Letzter funktionierender Zustand	Wann funktionierte der Dienst zuletzt nachweislich?
Betroffener Benutzer	Welcher Benutzer beobachtet das Problem?
Betroffenes Gerät	Hostname, Gerätetyp und Betriebssystem
Betroffener Dienst	Welche Anwendung, Verbindung oder Funktion ist gestört?
Standort	Gebäude, Raum, Homeoffice, Außenstelle oder Cloud
Netzwerkverbindung	Ethernet, WLAN, Mobilfunk oder VPN
Fehlermeldung	Exakter und vollständiger Wortlaut
Reproduzierbarkeit	Kann der Fehler gezielt erneut ausgelöst werden?
Häufigkeit	Dauerhaft, gelegentlich, periodisch oder einmalig
Auswirkung	Was kann der Benutzer oder das Unternehmen nicht durchführen?
Workaround	Gibt es einen vorübergehend funktionierenden Alternativweg?
Letzte Änderungen	Was wurde kurz vor dem Auftreten verändert?
Beweise	Screenshots, Logs, Zeitstempel, Monitoring oder Paketmitschnitt

---

Exakte Fehlermeldung erfassen

Fehlermeldungen dürfen nicht nur sinngemäß wiedergegeben werden.

Dokumentiert werden:

- vollständiger Wortlaut;
- Fehlercode;
- Event-ID;
- HTTP-Status;
- Uhrzeit;
- betroffene Anwendung;
- betroffener Vorgang;
- sichtbare Details;
- Screenshot, falls sinnvoll.

Beispiel:

Nicht ausreichend:

> Anmeldung geht nicht.

Besser:

> „Bei der Anmeldung erscheint um 08:14 Uhr die Meldung „Die Vertrauensstellung zwischen dieser Arbeitsstation und der primären Domäne konnte nicht hergestellt werden.“

Exakte Fehlermeldungen ermöglichen eine gezieltere Suche in Logs und Herstellerdokumentationen.

Zeitpunkt dokumentieren

Der genaue Zeitpunkt ist erforderlich, um Ereignisse verschiedener Systeme miteinander zu vergleichen.

Dokumentiert werden:

- Datum;
- Uhrzeit;
- Zeitzone;
- Beginn der Störung;
- letzter erfolgreicher Vorgang;
- Zeitpunkt jedes reproduzierten Fehlers.

Beispiel:

> „Fehler reproduziert am 30.07.2026 um 14:42:18 Uhr MESZ.

Ungefähre Angaben wie „heute Morgen“ oder „vorhin“ reichen für eine Logkorrelation nicht aus.

Zeit und Systeminformationen erfassen

Prüfung	Windows	Linux	macOS
Hostname	`[RO] hostname`	`[RO] hostname`	`[RO] hostname`
Benutzerkontext	`[RO] whoami`	`[RO] whoami`	`[RO] whoami`
Systemzeit	`[RO] Get-Date -Format o`	`[RO] date "+%Y-%m-%d %H:%M:%S %Z"`	`[RO] date "+%Y-%m-%d %H:%M:%S %Z"`

Prüfung	Windows	Linux	macOS
Betriebssystem	`[RO] Get-CimInstance Win32_OperatingSystem | Select-Object Caption,Version,BuildNumber`	`[RO] cat /etc/os-release`	`[RO] sw_vers`
Laufzeit	`[RO] (Get-Date) - (Get-CimInstance Win32_OperatingSystem).LastBootUpTime`	`[RO] uptime`	`[RO] uptime`
Letzter Systemstart	`[RO] Get-CimInstance Win32_OperatingSystem | Select-Object LastBootUpTime`	`[RO] who -b`	`[RO] sysctl -n kern.boottime`

Diese Befehle verändern keine Konfiguration.

Betroffenes System erfassen

Für einen Client oder Server werden mindestens folgende Angaben benötigt:

- Hostname;
- Gerätetyp;
- Hersteller und Modell, falls relevant;
- Betriebssystem;
- Betriebssystemversion;
- Patch- oder Buildstand;
- physisches Gerät, virtuelle Maschine oder Container;
- Standort;
- verwendete Netzwerkverbindung;
- Benutzerkontext;
- lokale oder zentrale Verwaltung;
- relevante Anwendungs- oder Dienstversion.

Betroffenen Dienst erfassen

Der betroffene Dienst muss möglichst genau benannt werden.

Nicht ausreichend:

> Der Server geht nicht.

Besser:

>

> Die HTTPS-Anwendung auf `app.example.internal` ist über TCP 443 nicht erreichbar. Der Server antwortet weiterhin auf ICMP und SSH.

Mögliche Dienstangaben:

- DNS;
- DHCP;
- HTTPS;
- SMB;
- RDP;
- SSH;
- VPN;
- Datenbank;
- Druckdienst;
- Active Directory;
- E-Mail;
- Containeranwendung;
- Cloud-Dienst;
- Netzwerkspeicher.

Sollzustand und Istzustand trennen

Zustand	Beschreibung
Sollzustand	Was sollte normalerweise geschehen?
Istzustand	Was geschieht tatsächlich?
Abweichung	Welcher konkrete Unterschied besteht?

Beispiel:

Zustand	Beobachtung
Sollzustand	Client erhält per DHCP eine Adresse aus `192.168.10.0/24`
Istzustand	Client verwendet `169.254.18.24/16`
Abweichung	Kein gültiger DHCP-Lease vorhanden

Reproduzierbarkeit dokumentieren

Ein reproduzierbarer Fehler ist leichter zu untersuchen als ein unregelmäßiger Fehler.

Dokumentiert werden:

1. Ausgangszustand;

2. genaue Aktion;
3. verwendeter Benutzer;
4. verwendetes Gerät;
5. Zielsystem oder Zieladresse;
6. erwartetes Ergebnis;
7. tatsächliches Ergebnis;
8. genaue Fehlerzeit.

Beispiel:

1. Client ist über Ethernet verbunden.
2. Benutzer öffnet `https://app.example.internal`.
3. Browser wartet ungefähr 30 Sekunden.
4. Anschließend erscheint ein Timeout.
5. Fehler reproduziert um 14:42:18 Uhr MESZ.
6. Andere Webseiten funktionieren.

Häufigkeit bestimmen

Auftreten	Dokumentation
Dauerhaft	Fehler tritt bei jedem Versuch auf
Gelegentlich	Fehler tritt unregelmäßig auf
Periodisch	Fehler tritt in erkennbaren Zeitabständen auf
Zeitabhängig	Fehler tritt nur zu bestimmten Uhrzeiten auf
Lastabhängig	Fehler tritt nur bei hoher Nutzung auf
Standortabhängig	Fehler tritt nur in einem Gebäude oder Netz auf
Benutzerabhängig	Fehler tritt nur mit einem bestimmten Konto auf
Geräteabhängig	Fehler tritt nur an einem bestimmten Client auf
Einmalig	Fehler konnte bisher nicht erneut erzeugt werden

Bei unregelmäßigen Fehlern müssen Zeitpunkt und Begleitumstände besonders genau dokumentiert werden.

Letzten funktionierenden Zustand festhalten

Die Frage lautet nicht nur:

> „Seit wann besteht der Fehler?

Zusätzlich muss geklärt werden:

> Wann wurde die betroffene Funktion zuletzt nachweislich erfolgreich verwendet?

Beispiele:

- letzte erfolgreiche Anmeldung;
- letzter erfolgreicher Druckauftrag;
- letzte erfolgreiche DNS-Abfrage;
- letzter erfolgreicher Backupjob;
- letzte erfolgreiche VPN-Verbindung;
- letzte erfolgreiche Replikation;
- letzter erfolgreicher API-Aufruf.

Der letzte funktionierende Zustand begrenzt den Zeitraum, in dem eine auslösende Änderung stattgefunden haben kann.

Letzte Änderungen erfassen

An dieser Stelle werden Änderungen zunächst nur gesammelt. Die technische Bewertung erfolgt später auf der Seite `1.3 Zeitpunkt und letzte Änderungen untersuchen`.

Mögliche Änderungen:

- Update oder Patch;
- Neustart;
- Treiber- oder Firmwareänderung;
- neue Anwendung;
- neue Hardware;
- Benutzer- oder Passwortänderung;
- Rechte- oder Gruppenänderung;
- GPO-Änderung;
- Firewall- oder ACL-Änderung;
- VLAN- oder Switchportänderung;
- Routing- oder NAT-Änderung;
- DNS- oder DHCP-Änderung;
- Zertifikatserneuerung;
- Migration;
- Snapshot oder Restore;
- Backupjob;
- Provider- oder Cloudänderung.

Auch die Antwort „Keine Änderung bekannt“ wird dokumentiert.

Auswirkung erfassen

Die technische Störung und ihre betriebliche Auswirkung sind getrennt zu dokumentieren.

Technische Störung	Mögliche Auswirkung
Ein Client erhält keine IP-Adresse	Ein Benutzer kann nicht arbeiten
DHCP für ein VLAN ausgefallen	Eine gesamte Abteilung erhält keine Netzwerkverbindung
DNS-Auflösung gestört	Mehrere Anwendungen erscheinen gleichzeitig ausgefallen
Fileserver nicht erreichbar	Gemeinsame Dokumente können nicht geöffnet werden
VPN ausgefallen	Remotezugriff für Außenstellen oder Homeoffice nicht möglich
Datenbank nicht erreichbar	Geschäftsanwendung vollständig ausgefallen
Backup fehlgeschlagen	Wiederherstellbarkeit möglicherweise gefährdet
Verdächtige Anmeldung	Möglicher Security-Vorfall

Workaround dokumentieren

Ein vorhandener Workaround kann bei der Eingrenzung helfen.

Beispiele:

- Ethernet funktioniert nicht, WLAN funktioniert;
- Hostname funktioniert nicht, direkte IP-Adresse funktioniert;
- VPN funktioniert nicht, lokaler Zugriff funktioniert;
- ein Browser funktioniert, ein anderer nicht;
- ein Benutzer ist betroffen, ein anderer nicht;
- ein Server ist betroffen, ein anderer Server funktioniert;
- Neustart behebt das Problem nur vorübergehend.

Ein Workaround ist keine dauerhafte Fehlerbehebung.

Beweise sichern

Mögliche Beweise:

- Screenshot;
- exportiertes Eventlog;
- Logdatei;
- Konsolenausgabe;
- Monitoringgraph;
- Prozessliste;
- Liste laufender Dienste;

- Netzwerkstatus;
- Interface-Counter;
- Routingtabelle;
- DNS-Ergebnis;
- Paketmitschnitt;
- Konfigurationsexport;
- Hersteller-Supportbundle.

Dateinamen sollten den Host und den Zeitpunkt enthalten.

Beispiel:

`client01_systemlog_2026-07-30_1442.evtx`

`server01_network_2026-07-30_1442.pcapng`

Sensible Daten, Passwörter, Tokens und private Schlüssel dürfen nicht ungeschützt in Tickets oder Dokumentationen eingefügt werden.

Vorlage für die Störungsaufnahme

Feld	Eintrag
Ticket oder Referenz	
Gemeldet von	
Aufgenommen am	
Aufgenommen durch	
Beginn der Störung	
Letzter funktionierender Zustand	
Betroffener Benutzer	
Betroffenes Gerät	
Hostname	
Betriebssystem und Version	
Standort	
Netzwerkverbindung	
Betroffener Dienst	
Zielsystem oder Zieladresse	
Sollzustand	
Istzustand	
Exakte Fehlermeldung	

Feld	Eintrag
Fehlercode oder Event-ID	
Reproduzierbar	
Schritte zur Reproduktion	
Häufigkeit	
Bekannte letzte Änderungen	
Betriebliche Auswirkung	
Vorhandener Workaround	
Gesicherte Logs und Beweise	
Genaue Fehlerzeit mit Zeitzone	
Security-Verdacht	
Zusätzliche Hinweise	

Beispiel einer ausgefüllten Störungsaufnahme

Feld	Eintrag
Ticket oder Referenz	INC-2026-0730-01
Gemeldet von	Benutzer der Arbeitsstation
Aufgenommen am	30.07.2026, 14:40 Uhr MESZ
Beginn der Störung	ungefähr 14:35 Uhr
Letzter funktionierender Zustand	30.07.2026, 12:10 Uhr
Betroffenes Gerät	Arbeitsplatzrechner
Hostname	CLIENT-01
Betriebssystem und Version	Windows 11
Standort	Hauptstandort, Raum 204
Netzwerkverbindung	Ethernet
Betroffener Dienst	DHCP und allgemeiner Netzwerkzugriff
Sollzustand	IPv4-Adresse aus `192.168.10.0/24`
Istzustand	IPv4-Adresse `169.254.18.24/16`
Exakte Fehlermeldung	Keine Fehlermeldung angezeigt
Reproduzierbar	Ja
Häufigkeit	Dauerhaft über Ethernet
Bekannte letzte Änderungen	Keine Änderung bekannt

Feld	Eintrag
Betriebliche Auswirkung	Benutzer kann keine internen Dienste erreichen
Vorhandener Workaround	WLAN funktioniert
Gesicherte Beweise	Ausgabe von `ipconfig /all`, Screenshot und Fehlerzeit
Security-Verdacht	Nein

Diese Aufnahme beschreibt den Zustand. Die technische Eingrenzung erfolgt anschließend auf der Seite `1.2 Fehlerumfang mit Kreuztests bestimmen`.

Ungeeignete Störungsbeschreibungen

- „Geht nicht.“
- „Alles ist langsam.“
- „Seit dem Update ist alles kaputt.“
- „Der Server ist offline.“
- „DNS ist defekt.“
- „Die Firewall blockiert.“
- „Der Benutzer macht etwas falsch.“
- „Nach einem Neustart geht es wieder.“

Diese Aussagen enthalten Vermutungen oder sind technisch nicht ausreichend eingegrenzt.

Ergebnis dieser Seite

Nach Abschluss der Störungsaufnahme müssen folgende Punkte bekannt sein:

- sichtbares Symptom;
- Sollzustand;
- Istzustand;
- exakte Fehlermeldung;
- betroffener Benutzer;
- betroffenes Gerät;
- betroffener Dienst;
- Beginn der Störung;
- letzter funktionierender Zustand;
- Reproduzierbarkeit;
- Häufigkeit;
- bekannte Änderungen;
- betriebliche Auswirkung;
- möglicher Workaround;
- vorhandene Logs und Beweise.

Erst danach beginnt die systematische technische Eingrenzung.

Nächste Seite

1.2 Fehlerumfang mit Kreuztests bestimmen

Quellen

- IBM – Systematischer Troubleshooting-Ansatz
- Microsoft – Windows Networking Troubleshooting
- Microsoft – DHCP Troubleshooting Checklist
- Microsoft – Windows Performance Troubleshooting
- NIST – Incident Response Recommendations