3.5 Auswirkungen, Dringlichkeit und Priorität

> **Kurz erklärt**
>
> Die Priorität bestimmt, in welcher Reihenfolge und mit welcher Aufmerksamkeit ein Vorgang bearbeitet werden soll.
>
> Sie sollte nicht allein davon abhängen:
>
> - wer am lautesten fordert,
> - wer hierarchisch am höchsten steht,
> - wann das Ticket erstellt wurde,
> - oder welche Priorität ein Benutzer selbst auswählt.
>
> Eine verbreitete betriebliche Vorgehensweise ist, die Priorität anhand von:
>
> - **Auswirkung**
> - und **Dringlichkeit**
>
> zu bestimmen.
>
> **Auswirkung** beschreibt, wie stark Benutzer, Services, Geschäftsprozesse oder andere Stakeholder beeinträchtigt sind.
>
> **Dringlichkeit** beschreibt, wie schnell gehandelt werden muss, bevor sich die Folgen verschlimmern oder ein wichtiges Zeitfenster verloren geht.
>
> Die Organisation muss selbst festlegen:
>
> - welche Bewertungsstufen gelten,
> - welche Kriterien verwendet werden,
> - wie daraus eine Priorität entsteht,
> - welche Zielzeiten damit verbunden sind,
> - wer die Priorität ändern darf,
> - und wann eine Neubewertung erfolgen muss.
>
> ITIL schreibt keine universelle Prioritätsmatrix vor, die unverändert für jede Organisation übernommen werden kann.

Warum eine nachvollziehbare Priorisierung notwendig ist

Eine Serviceorganisation besitzt normalerweise mehr offene Arbeit, als gleichzeitig bearbeitet werden kann.

Beispiele:

- mehrere Benutzer melden unterschiedliche Incidents,
- Service Requests warten auf Erfüllung,
- Lieferanten müssen eingebunden werden,
- Changes benötigen technische Vorbereitung,
- und bereits laufende Vorgänge benötigen weitere Maßnahmen.

Ohne nachvollziehbare Priorisierung kann die Reihenfolge bestimmt werden durch:

- persönliche Beziehungen,
- häufige Nachfragen,
- Hierarchie,
- Zufall,
- technische Vorlieben,
- oder das Alter des Tickets.

Dadurch können schwerwiegende Situationen übersehen werden, während weniger bedeutsame Vorgänge bevorzugt bearbeitet werden.

Beispiel:

Vorgang A

Ein Vorstandsmitglied kann einen zweiten, selten verwendeten Bildschirm nicht nutzen.

Vorgang B

Ein einzelner Produktionsarbeitsplatz kann keine Sicherheitsfreigaben mehr durchführen. Dadurch steht in 20 Minuten eine gesamte Fertigungslinie still.

Obwohl bei beiden Vorgängen zunächst nur eine Person betroffen ist, besitzt Vorgang B wahrscheinlich die deutlich größere Auswirkung und Dringlichkeit.

> **Merke**
>
> Priorisierung bewertet nicht die persönliche Wichtigkeit eines Benutzers.
>
> Sie bewertet die Bedeutung und zeitliche Kritikalität des betroffenen Outcomes.

Auswirkung, Dringlichkeit und Priorität unterscheiden

Begriff	Zentrale Frage

Auswirkung	Wie schwerwiegend sind die Folgen für Benutzer, Services oder Organisation?
Dringlichkeit	Wie schnell muss gehandelt werden, bevor die Folgen unvertretbar werden?
Priorität	In welcher Reihenfolge und mit welcher Aufmerksamkeit wird der Vorgang bearbeitet?

Beispiel:

Ein Archivsystem ist ausgefallen.

Mögliche geringe Dringlichkeit

- Das System wird erst in drei Tagen benötigt.
- Eine sichere alternative Zugriffsmöglichkeit besteht.
- Es droht kein Datenverlust.

Mögliche hohe Auswirkung

- Das System enthält geschäftskritische und gesetzlich aufzubewahrende Unterlagen.
- Viele Bereiche sind davon abhängig.

Die Auswirkung kann damit hoch sein, während die unmittelbare Dringlichkeit zunächst geringer ist.

Ein anderes Beispiel:

Ein einzelner Benutzer kann eine Präsentation für einen in zehn Minuten beginnenden Kundentermin nicht öffnen.

- Auswirkung auf die gesamte Organisation möglicherweise begrenzt
- Dringlichkeit aufgrund des unmittelbar bevorstehenden Termins hoch

> **Wichtig**
>
> Auswirkung und Dringlichkeit beschreiben unterschiedliche Perspektiven.
>
> Eine hohe Auswirkung bedeutet nicht automatisch höchste Dringlichkeit.

Priorität ist keine technische Fehlerklasse

Ein technisch kleiner Fehler kann eine hohe geschäftliche Priorität besitzen.

Beispiel:

Ein abgelaufenes Zertifikat ist möglicherweise schnell erneuerbar.

Wenn dadurch jedoch:

- die zentrale Anmeldung ausfällt,
- sämtliche Benutzer betroffen sind,
- und kein sicherer Workaround besteht,

kann der Incident höchste Priorität erhalten.

Umgekehrt kann ein technisch komplexes Problem eine geringere Priorität besitzen.

Beispiel:

Ein selten verwendeter Bericht erzeugt unter einer bestimmten Kombination von Filtern einen Darstellungsfehler.

Die Analyse kann technisch aufwendig sein.

Wenn jedoch:

- keine wichtigen Daten verloren gehen,
- nur wenige Benutzer betroffen sind,
- und eine einfache Alternative besteht,

kann eine niedrigere Priorität angemessen sein.

> **Merke**
>
> Technische Schwierigkeit und betriebliche Priorität sind nicht dasselbe.

Mögliche Einflussfaktoren auf die Auswirkung

Die Organisation kann mehrere Kriterien berücksichtigen.

Anzahl betroffener Benutzer

Mögliche Abstufung:

- einzelne Person
- mehrere Personen
- gesamtes Team
- gesamter Standort
- mehrere Standorte

- sämtliche Benutzer
- externe Kunden oder Partner

Die Anzahl allein reicht jedoch nicht aus.

Ein einzelner betroffener Benutzer kann eine kritische Aufgabe ausführen.

Kritikalität des betroffenen Service

Beispiele:

- zentrale Anmeldung
- Produktionssteuerung
- Notfallkommunikation
- Zahlungsverkehr
- E-Mail
- Dateiablage
- internes Testsystem
- freiwillige Zusatzanwendung

Die Organisation sollte wichtige Services und deren Abhängigkeiten kennen.

Bedeutung des betroffenen Geschäftsprozesses

Mögliche Auswirkungen:

- Produktion steht still.
- Rechnungen können nicht erstellt werden.
- Kunden können nicht bestellen.
- Personal kann keine Gehaltsabrechnung durchführen.
- gesetzliche Meldung kann nicht fristgerecht übermittelt werden.
- Außendienst kann keine Aufträge erfassen.
- interne Schulungsplattform ist vorübergehend nicht erreichbar.

Art der Beeinträchtigung

Beeinträchtigung	Beispiel
vollständiger Ausfall	Service ist nicht nutzbar
teilweiser Ausfall	bestimmte Funktionen fehlen
Leistungsminderung	Service reagiert stark verzögert
Qualitätsminderung	Ergebnisse sind unvollständig oder fehlerhaft
Sicherheitsbeeinträchtigung	Schutzbedarf könnte verletzt sein
Datenbeeinträchtigung	Daten sind verloren, beschädigt oder inkonsistent

Beeinträchtigung	Beispiel
Erfahrungsbeeinträchtigung	Service ist technisch verfügbar, aber praktisch kaum nutzbar

Verfügbarkeit einer Zwischenlösung

Eine geeignete Zwischenlösung kann die Auswirkung oder Dringlichkeit reduzieren.

Beispiele:

- alternativer Arbeitsplatz
- Webversion statt Desktop-Anwendung
- zweiter Drucker
- manuelle Ersatzbearbeitung
- Ausweichstandort
- vorübergehender Read-only-Zugriff
- alternative Kommunikationsplattform

Die Zwischenlösung muss jedoch:

- sicher,
- zulässig,
- ausreichend leistungsfähig,
- verständlich,
- und für die betroffenen Benutzer tatsächlich nutzbar

sein.

Ungeeignet wäre beispielsweise:

> „ Benutzer können ihre Dokumente an private E-Mail-Adressen senden.

Auch wenn dadurch kurzfristig weitergearbeitet werden könnte, wäre dies möglicherweise aus Sicherheits- und Datenschutzgründen unzulässig.

Dauer und Reichweite

Die tatsächliche Auswirkung kann mit der Zeit wachsen.

Beispiel:

Ein Bestellsystem fällt am frühen Morgen aus.

Zu Beginn bestehen nur wenige offene Bestellungen.

Nach mehreren Stunden können entstehen:

- wachsender Rückstand,
- verpasste Liefertermine,
- Kundenbeschwerden,
- und finanzielle Schäden.

Die Priorität muss deshalb möglicherweise während der Bearbeitung erhöht werden.

Finanzielle Auswirkungen

Mögliche Kriterien:

- Umsatzverlust
- Produktionsstillstand
- Vertragsstrafe
- zusätzliche Personalkosten
- kostenpflichtige Notfallunterstützung
- verlorene Arbeitszeit
- drohender Kundenverlust

Nicht jede Organisation kann exakte Beträge während der Ersterfassung bestimmen.

Eine qualitative Bewertung kann zunächst ausreichen.

Sicherheits- und Datenschutzfolgen

Mögliche Auswirkungen:

- unberechtigter Zugriff
- Offenlegung vertraulicher Daten
- Verlust der Verfügbarkeit
- Veränderung von Daten
- Schadsoftware
- kompromittiertes Konto
- verlorenes Gerät
- unsichere technische Konfiguration

Ein möglicher Sicherheitsvorfall benötigt möglicherweise:

- eine eigene Klassifizierung,
- einen besonders geschützten Bearbeitungsweg,
- und eine sofortige Eskalation.

Er darf nicht ausschließlich anhand der Zahl aktuell betroffener Benutzer bewertet werden.

Gesetzliche und regulatorische Auswirkungen

Mögliche Beispiele:

- Meldefrist wird gefährdet.
- gesetzlich vorgeschriebene Aufzeichnung ist nicht möglich.
- Aufbewahrungspflichten könnten verletzt werden.
- personenbezogene Daten wurden möglicherweise offengelegt.

Die Organisation muss ihre verbindlichen Anforderungen kennen und in die Bewertung einbeziehen.

Auswirkungen auf Kunden, Öffentlichkeit und Reputation

Mögliche Folgen:

- Kunden können Leistungen nicht nutzen.
- öffentliche Statusseiten zeigen einen Ausfall.
- Medien oder soziale Netzwerke berichten über die Störung.
- vertraglich zugesagte Leistungen werden nicht erbracht.
- Vertrauen in die Organisation sinkt.

Reputationsauswirkung sollte nicht nur nach subjektivem Eindruck bewertet werden.

Geeignete Eskalations- und Kommunikationsrollen müssen beteiligt werden.

Auswirkungen auf Gesundheit und Sicherheit

In bestimmten Umgebungen können IT-Störungen Auswirkungen besitzen auf:

- körperliche Sicherheit,
- medizinische Versorgung,
- Gebäudezugänge,
- Notfallkommunikation,
- Maschinensteuerung,
- oder sicherheitskritische Überwachung.

Solche Situationen benötigen möglicherweise:

- besonders schnelle Eskalation,
- Notfallverfahren,
- Business-Continuity-Maßnahmen,
- und autorisierte Entscheidungen außerhalb des normalen Supportablaufs.

Mögliche Einflussfaktoren auf die Dringlichkeit

Dringlichkeit beschreibt die verfügbare Zeit bis zu einer wesentlichen Verschlechterung oder bis zum Verlust eines wichtigen Outcomes.

Unmittelbarer Zeitdruck

Beispiele:

- Produktion steht bereits still.
- Kunden können aktuell nicht bestellen.
- ein gesetzlicher Meldetermin endet heute.
- ein wichtiger Geschäftstermin beginnt in wenigen Minuten.
- Sicherheitslücke wird aktiv ausgenutzt.
- Datenverlust setzt sich fort.

Zeit bis zur erwarteten Verschlechterung

Beispiel:

Ein Speicherbereich ist zu 95 Prozent belegt.

Der Service funktioniert noch.

Monitoring zeigt jedoch, dass der Speicher voraussichtlich innerhalb einer Stunde vollständig belegt sein wird.

Obwohl noch kein vollständiger Ausfall besteht, kann hohe Dringlichkeit vorliegen.

Verbleibendes Zeitfenster

Beispiele:

- Wartungsfenster endet in 30 Minuten.
- Lieferantensupport ist nur noch eine Stunde erreichbar.
- Abrechnungslauf beginnt am Abend.
- Zertifikat läuft in zwei Tagen ab.
- Produktionsumstellung beginnt am nächsten Morgen.
- Backup-Zeitfenster endet vor Schichtbeginn.

Verfügbarkeit einer Zwischenlösung

Eine sichere und praktikable Zwischenlösung kann die Dringlichkeit reduzieren.

Beispiel:

Die Desktop-Anwendung ist ausgefallen.

Die Webversion ermöglicht alle wichtigen Tätigkeiten.

Die Bearbeitung kann dadurch möglicherweise kontrollierter erfolgen.

Die Zwischenlösung muss allerdings hinsichtlich folgender Punkte bewertet werden:

- Leistungsfähigkeit
- Benutzerzahl
- Sicherheit
- Dauer
- Datenkonsistenz
- zusätzlicher Aufwand
- mögliche Folgefehler

Drohender Datenverlust

Dringlichkeit kann besonders hoch sein, wenn:

- Daten weiterhin überschrieben werden,
- Speicherfehler weitere Dateien beschädigen,
- gelöschte Daten nur begrenzte Zeit wiederherstellbar sind,
- oder Logs und Beweise verloren gehen könnten.

In solchen Situationen kann die erste Maßnahme darin bestehen:

- weitere Veränderungen zu verhindern,
- Systeme zu isolieren,
- Beweise zu sichern,
- oder Schreibzugriffe zu stoppen.

Eine vorschnelle normale Fehlerbehebung kann Wiederherstellungsmöglichkeiten verschlechtern.

Sicherheitsbedrohung

Hohe Dringlichkeit kann vorliegen bei:

- aktivem Angriff,
- kompromittiertem Administratorkonto,
- laufender Datenübertragung an Unberechtigte,
- Schadsoftwareausbreitung,
- oder bekanntem ungeschütztem kritischem Zugang.

Die Bearbeitung richtet sich dann nicht nur nach Incident Management, sondern auch nach dem Sicherheitsverfahren der Organisation.

Kommender geschäftskritischer Zeitpunkt

Beispiel:

Die Gehaltsabrechnung funktioniert am Montag nicht.

Der endgültige Abrechnungslauf beginnt erst am Mittwoch.

Die Auswirkung ist bereits erheblich.

Die verfügbare Zeit bis Mittwoch beeinflusst jedoch die Dringlichkeit und den möglichen Eskalationsweg.

Eine mögliche Auswirkungsskala

Die folgende Skala ist ein redaktionelles Beispiel.

Sie ist keine verbindliche ITIL-Vorgabe.

Stufe	Beispielhafte Bedeutung
Hoch	kritischer Service, großer Benutzerkreis, erheblicher Geschäfts-, Sicherheits- oder Kundenbezug
Mittel	mehrere Benutzer oder wichtiger Teil eines Service betroffen, begrenzte Zwischenlösung vorhanden
Niedrig	einzelne oder wenige Benutzer, begrenzte Folgen, geeignete Alternative vorhanden

Eine Organisation kann stattdessen verwenden:

- vier Stufen,
- fünf Stufen,
- numerische Werte,
- serviceabhängige Kriterien,
- oder ein anderes nachvollziehbares Modell.

Beispielkriterien für hohe Auswirkung

Eine hohe Auswirkung kann beispielsweise vorliegen, wenn mindestens eines der folgenden Kriterien erfüllt ist:

- kritischer Service vollständig ausgefallen
- mehrere Standorte betroffen
- wichtiger Geschäftsprozess gestoppt
- erheblicher Kundenbezug
- mögliches erhebliches Sicherheits- oder Datenschutzereignis
- erheblicher Datenverlust
- Gesundheits- oder Sicherheitsrisiko
- keine geeignete Zwischenlösung
- erhebliche finanzielle oder vertragliche Folgen

Die Organisation muss festlegen, ob:

- ein einzelnes Kriterium ausreicht,
- mehrere Kriterien gemeinsam erfüllt sein müssen,
- oder eine autorisierte Rolle die Gesamtbewertung vornimmt.

Eine mögliche Dringlichkeitsskala

Auch diese Skala ist ein redaktionelles Beispiel.

Stufe	Beispielhafte Bedeutung
Hoch	sofortiges Handeln erforderlich; Folgen treten bereits ein oder verschlimmern sich sehr schnell
Mittel	zeitnahe Bearbeitung erforderlich; begrenztes Zeitfenster oder zunehmende Folgen
Niedrig	Bearbeitung planbar; Auswirkungen verschlechtern sich voraussichtlich nicht kurzfristig

---

Beispielkriterien für hohe Dringlichkeit

- Service steht bereits vollständig still.
- Schaden nimmt fortlaufend zu.
- Sicherheitsbedrohung ist aktiv.
- Datenverlust setzt sich fort.
- kritische Frist läuft kurzfristig ab.
- keine geeignete Zwischenlösung besteht.
- Wiederherstellungszeitfenster wird bald überschritten.
- weitere Services könnten kurzfristig ausfallen.

Eine mögliche Prioritätsmatrix

Die folgende Matrix ist eine Praxisvorlage und keine verbindliche ITIL-Matrix.

Auswirkung	Dringlichkeit hoch	Dringlichkeit mittel	Dringlichkeit niedrig
hoch	P1	P2	P3
mittel	P2	P3	P4
niedrig	P3	P4	P4

Eine Organisation kann auch andere Ergebnisse festlegen.

Beispielsweise könnte:

- hohe Auswirkung und niedrige Dringlichkeit als P2 behandelt werden,
- jeder mögliche Sicherheitsvorfall automatisch einen besonderen Eskalationsweg erhalten,

- oder ein kritischer Service eigene Prioritätsregeln besitzen.

> **Wichtig**
>
> Eine Matrix unterstützt Entscheidungen.
>
> Sie ersetzt nicht die fachliche Bewertung besonderer Situationen.

Mögliche Prioritätsstufen

Priorität	Praxisnahe Bedeutung
P1 – kritisch	sofortige koordinierte Bearbeitung; sehr hohe Auswirkung und Dringlichkeit
P2 – hoch	schnelle priorisierte Bearbeitung; erhebliche Beeinträchtigung
P3 – mittel	normale priorisierte Bearbeitung innerhalb vereinbarter Ziele
P4 – niedrig	planbare Bearbeitung bei begrenzter Auswirkung und Dringlichkeit

Manche Organisationen verwenden:

- P0 bis P4,
- Priorität 1 bis 5,
- Kritisch, Hoch, Mittel, Niedrig,
- Severity-Level,
- oder serviceabhängige Modelle.

Die Bedeutung muss eindeutig dokumentiert sein.

Priorität und Severity unterscheiden

Der Begriff **Severity** wird in Organisationen unterschiedlich verwendet.

Mögliche Bedeutungen:

- technische Schwere eines Fehlers,
- Ausmaß der Servicebeeinträchtigung,
- Softwarefehlerklasse,
- oder Einstufung eines Sicherheitsereignisses.

Priorität beschreibt dagegen die Bearbeitungsreihenfolge und Aufmerksamkeit.

Beispiel:

Ein Softwarefehler kann hohe Severity besitzen, weil er bei bestimmten Bedingungen Daten beschädigt.

Wenn diese Funktion derzeit deaktiviert ist und kein unmittelbarer Schaden droht, kann die operative Bearbeitungspriorität zunächst anders eingeordnet werden.

> **Praxistipp**
>
> Die Organisation sollte in einem Glossar eindeutig festlegen, wie Severity und Priorität verwendet werden.

Priorität und Servicekritikalität unterscheiden

Servicekritikalität ist eine grundsätzlichere Eigenschaft eines Service.

Beispiele:

- geschäftskritisch
- wichtig
- unterstützend
- nicht produktiv

Die Priorität bewertet dagegen einen konkreten Vorgang.

Ein Incident an einem kritischen Service besitzt nicht automatisch immer P1.

Beispiel:

In einer geschäftskritischen Anwendung ist nur eine selten verwendete Berichtsfunktion betroffen.

Der Kernservice funktioniert.

Eine geeignete Zwischenlösung besteht.

Der konkrete Incident kann deshalb eine niedrigere Priorität erhalten.

Umgekehrt kann ein normalerweise weniger kritischer Service zu einem bestimmten Zeitpunkt besonders wichtig sein.

Beispiel:

Eine Schulungsplattform wird während einer verbindlichen Abschlussprüfung benötigt.

Priorität und Major Incident unterscheiden

Ein Major Incident ist ein Incident mit besonders erheblicher Bedeutung, der eine besondere Koordination und Kommunikation erfordern kann.

Eine Organisation legt eigene Kriterien fest.

Ein P1-Incident kann ein Major Incident sein.

Dies muss jedoch nicht in jeder Organisation automatisch identisch sein.

Priorität	Major Incident
bestimmt Bearbeitungsreihenfolge und Zielzeiten	aktiviert besondere Koordination und Kommunikation
kann für unterschiedliche Vorgangsarten gelten	bezieht sich auf besonders schwerwiegende Incidents
wird häufig aus Auswirkung und Dringlichkeit bestimmt	kann zusätzliche definierte Kriterien besitzen
kann durch normale Supportstruktur bearbeitet werden	benötigt möglicherweise Incident-Koordination, Krisenkommunikation und Managementbeteiligung

Major-Incident-Kriterien werden auf Seite **3.7 Ownership, hierarchische Eskalation und Major Incidents** vertieft.

Priorität und Eskalation unterscheiden

Hohe Priorität kann eine Eskalation auslösen.

Eine Eskalation kann jedoch auch notwendig sein, wenn die Priorität nicht besonders hoch ist.

Beispiele:

- Zielzeit ist gefährdet.
- zuständige Fachkenntnis fehlt.
- Lieferant reagiert nicht.
- Entscheidung liegt außerhalb vorhandener Befugnisse.
- mehrere Teams sind uneinig.
- Benutzerbeschwerde benötigt Managementbeteiligung.
- regulatorische Frage muss geklärt werden.

Die Priorität beschreibt nicht vollständig, welcher Eskalationstyp benötigt wird.

Priorität und Zielzeiten unterscheiden

Prioritätsstufen können mit unterschiedlichen Zielen verbunden sein.

Mögliche Ziele:

- Zeit bis zur Annahme
- Zeit bis zur qualifizierten Reaktion
- Zeit bis zum Beginn der Bearbeitung
- Zeit bis zur Wiederherstellung
- Zeit bis zur Erfüllung
- Statusintervall
- Eskalationszeitpunkt

Beispielhafte interne Ziele:

Priorität	Qualifizierte Reaktion	Statusintervall
P1	unverzüglich	alle 30 Minuten
P2	innerhalb einer Stunde	alle 2 Stunden
P3	innerhalb eines Arbeitstags	nach wesentlichen Änderungen
P4	nach Planung	nach Vereinbarung

Diese Werte sind nur Beispiele.

Die tatsächlichen Ziele müssen zu:

- Servicezeiten,
- Verträgen,
- Servicekritikalität,
- Fähigkeiten,
- Bereitschaft,
- und verfügbaren Ressourcen

passen.

Reaktionsziel ist kein Lösungsversprechen

Eine Zielzeit für die erste Reaktion bedeutet nicht automatisch, dass der Incident innerhalb dieses Zeitraums gelöst sein muss.

Beispiel:

> “ Qualifizierte Reaktion innerhalb von 30 Minuten

kann bedeuten:

- Situation wurde bewertet,
- Ownership wurde übernommen,

- erste Diagnose hat begonnen,
- und Benutzer erhielt eine verwertbare Rückmeldung.

Eine Wiederherstellungszeit hängt unter anderem ab von:

- Ursache,
- technischer Komplexität,
- Abhängigkeiten,
- Lieferanten,
- und verfügbaren Wiederherstellungsoptionen.

> **Merke**
>
> Serviceziele müssen verständlich benannt werden.
>
> „Antwort innerhalb einer Stunde“ darf nicht als „Lösung innerhalb einer Stunde“ missverstanden werden.

Statusintervalle nach Priorität

Bei hoher Priorität benötigen Stakeholder häufigere Informationen.

Ein Statusintervall sollte festlegen:

- wie oft informiert wird,
- wer informiert,
- welche Zielgruppen informiert werden,
- und welcher Kanal verwendet wird.

Auch wenn keine neue Lösung vorliegt, kann eine Statusmeldung enthalten:

- was aktuell geprüft wird,
- welche Maßnahmen bereits erfolgten,
- welche Abhängigkeit besteht,
- welche Zwischenlösung gilt,
- und wann die nächste Information folgt.

Priorität bei der Ersterfassung

Bei der ersten Meldung liegen häufig noch nicht alle Informationen vor.

Eine vorläufige Priorität kann anhand der verfügbaren Angaben gesetzt werden.

Danach sollte sie überprüft werden, sobald bekannt ist:

- wie viele Benutzer betroffen sind,
- welcher Service tatsächlich beeinträchtigt ist,
- ob eine Zwischenlösung besteht,
- ob weitere Standorte betroffen sind,
- und ob Sicherheits- oder Datenrisiken bestehen.

> **Wichtig**
>
> Eine erste Priorität ist keine unveränderliche Entscheidung.

Priorität dynamisch neu bewerten

Eine Neubewertung ist sinnvoll, wenn:

- weitere Benutzer betroffen sind,
- die Störung sich ausbreitet,
- eine Zwischenlösung ausfällt,
- ein kritischer Termin näher rückt,
- Datenverlust erkannt wird,
- ein Sicherheitsbezug entsteht,
- der Service vollständig ausfällt,
- oder die Wiederherstellung länger dauert als erwartet.

Die Priorität kann auch gesenkt werden, wenn:

- ein wirksamer Workaround eingeführt wurde,
- nur eine weniger wichtige Funktion betroffen ist,
- oder sich die ursprüngliche Auswirkung als geringer herausstellt.

Jede wesentliche Änderung sollte dokumentiert werden.

Prioritätsänderungen dokumentieren

Eine nachvollziehbare Dokumentation kann enthalten:

- alte Priorität
- neue Priorität
- Zeitpunkt
- Grund
- entscheidende Rolle
- geänderte Auswirkung oder Dringlichkeit

- ausgelöste Eskalation
- Kommunikationsmaßnahme

Beispiel:

> 10:25 Uhr – Priorität von P3 auf P1 erhöht. Ursprünglich war ein einzelner Arbeitsplatz betroffen. Inzwischen können sämtliche Benutzer des Standorts keine Produktionsfreigabe durchführen. Fertigung steht seit 10:20 Uhr. Incident-Koordination und Standortleitung wurden informiert.

Wer darf die Priorität ändern?

Die Organisation sollte festlegen:

- wer initial priorisiert,
- wer eine Priorität erhöhen darf,
- wer sie reduzieren darf,
- wann Management oder Service Owner beteiligt werden,
- und wie Konflikte entschieden werden.

Mögliche Rollen:

- Service Desk
- Incident Manager
- Service Owner
- technische Supportgruppe
- Informationssicherheit
- autorisierte Führungskraft

Eine Priorität darf nicht allein deshalb geändert werden, weil eine Person eine schnellere Bearbeitung verlangt.

Benutzerwunsch und organisatorische Priorität

Benutzer sollen die Auswirkungen und zeitlichen Anforderungen beschreiben können.

Sie müssen jedoch nicht zwingend die endgültige Priorität auswählen.

Eine geeignete Kommunikation kann lauten:

>

> Sie haben angegeben, dass die Angelegenheit sehr dringend ist. Ich prüfe jetzt zusätzlich, wie viele Benutzer und welcher Geschäftsprozess betroffen sind. Daraus wird die Priorität nach unseren Kriterien bestimmt.

Bei abweichender Bewertung:

> Ich verstehe, dass Sie die Anwendung heute benötigen. Da aktuell nur eine Person betroffen ist, eine sichere Alternative besteht und keine Frist innerhalb der nächsten Stunden gefährdet ist, wird der Vorgang als P3 bearbeitet. Sollte die Alternative ausfallen oder der Monatsabschluss gefährdet sein, bewerten wir die Priorität erneut.

Hierarchie ist kein automatisches Prioritätskriterium

Ein Vorgang einer Führungskraft kann hohe Auswirkung besitzen.

Beispiel:

Die Person muss eine zeitkritische strategische Entscheidung freigeben.

Die hierarchische Position allein genügt jedoch nicht als Begründung.

Ungeeignet:

> Tickets der Geschäftsführung sind immer P1.

Besser:

- geschäftliche Auswirkungen erfassen,
- Dringlichkeit bestimmen,
- organisatorische Kriterien anwenden,
- und gegebenenfalls besondere Kommunikationsanforderungen berücksichtigen.

> **Grundsatz**
>
> Eine besondere Kommunikationsbehandlung ist nicht automatisch eine höhere technische Bearbeitungspriorität.

VIP-Regelungen kritisch gestalten

Organisationen verwenden teilweise VIP-Kennzeichnungen.

Diese können unterstützen bei:

- besonderen Kommunikationswegen,
- Assistenzkontakten,
- erweiterten Servicezeiten,
- oder organisatorisch vereinbarten Leistungen.

Sie sollten nicht dazu führen, dass:

- kritische Incidents anderer Benutzer verdrängt werden,
- Sicherheitsprüfungen entfallen,
- oder Prioritätskriterien bedeutungslos werden.

Zwischenlösungen richtig bewerten

Ein Workaround reduziert möglicherweise die Dringlichkeit.

Er löst jedoch nicht automatisch den Incident dauerhaft.

Beispiel:

Die Desktop-Anwendung ist ausgefallen.

Benutzer können vorübergehend die Webversion verwenden.

Zu prüfen ist:

- Sind alle benötigten Funktionen vorhanden?
- Können sämtliche betroffenen Benutzer sie nutzen?
- Ist die Lösung sicher?
- Entsteht zusätzlicher Aufwand?
- Wie lange ist der Workaround tragfähig?
- Werden Daten konsistent verarbeitet?

Ein Workaround kann damit:

- Priorität senken,
- Zeit für Ursachenanalyse schaffen,
- oder Auswirkungen begrenzen.

Er darf aber nicht unkritisch als vollständige Lösung behandelt werden.

Priorisierung bei mehreren gleichzeitig kritischen Incidents

Mehrere P1-Incidents können gleichzeitig auftreten.

Dann reicht die Prioritätsnummer allein möglicherweise nicht aus.

Zusätzlich zu bewerten sind:

- Gesundheits- und Sicherheitsrisiken
- aktive Sicherheitsbedrohung
- Datenverlust
- Anzahl und Bedeutung betroffener Services
- verfügbare Wiederherstellungsmöglichkeiten
- Abhängigkeiten
- benötigte Spezialisten
- mögliche Kettenreaktionen

Governance oder Incident-Koordination muss möglicherweise Ressourcen zwischen den Vorgängen verteilen.

Abhängige Services berücksichtigen

Ein Incident kann zunächst nur eine technische Komponente betreffen.

Diese kann jedoch mehrere Services unterstützen.

Beispiel:

Ein zentraler Identitätsdienst zeigt erste Fehler.

Aktuell ist nur eine interne Anwendung betroffen.

Möglicherweise werden kurz darauf ebenfalls beeinträchtigt:

- E-Mail,
- VPN,
- Cloud-Anwendungen,
- Administrationszugänge,
- und Self-Service-Portal.

Die Priorität sollte potenzielle und bekannte Abhängigkeiten berücksichtigen, ohne unbelegte Worst-Case-Annahmen als Tatsache zu behandeln.

Verknüpfte Incidents gemeinsam betrachten

Mehrere scheinbar unabhängige Meldungen können einen gemeinsamen Auslöser besitzen.

Beispiele:

- Anmeldung funktioniert nicht.
- VPN-Verbindung schlägt fehl.
- Cloud-Anwendung öffnet nicht.
- Kennwort-Self-Service ist nicht erreichbar.

Wenn alle Services vom gleichen Identitätsdienst abhängen, kann ein gemeinsamer Incident mit höherer Auswirkung vorliegen.

Service Requests priorisieren

Nicht nur Incidents benötigen eine Bearbeitungsreihenfolge.

Auch Service Requests können unterschiedliche Dringlichkeit und Bedeutung besitzen.

Beispiele:

- Standardsoftware für einen zukünftigen Arbeitsplatz
- Zugriff für neuen Mitarbeiter
- Bestellung eines Ersatzgeräts
- Berechtigung für einen zeitkritischen Projekteinsatz
- Information zu einem Service

Service Requests sollten trotzdem nicht wie Incidents behandelt werden.

Bei Requests können zusätzlich relevant sein:

- gewünschter Bereitstellungstermin
- Genehmigungsstatus
- Standardbereitstellungszeit
- Verfügbarkeit von Lizenzen oder Assets
- vertragliche oder organisatorische Verpflichtung

Eine verspätet eingereichte Anfrage wird nicht automatisch zum Incident.

Beispiel:

Eine Führungskraft beantragt erst am Freitagnachmittag einen vollständigen Arbeitsplatz für Montag.

Die Anfrage ist dringend.

Es liegt jedoch nicht zwingend eine ungeplante Serviceunterbrechung vor.

Notfall durch schlechte Planung

Eine intern verspätete Anfrage sollte nicht automatisch höchste technische Priorität erhalten.

Trotzdem muss die Organisation die tatsächlichen Auswirkungen berücksichtigen.

Geeignete Vorgehensweise:

- Request korrekt klassifizieren,
- mögliche Beschleunigung prüfen,
- Risiken und Zusatzaufwand transparent machen,
- notwendige Entscheidungen eskalieren,
- und wiederkehrende Planungsprobleme verbessern.

Backlog und Priorität

Innerhalb derselben Priorität kann die Reihenfolge zusätzlich bestimmt werden durch:

- Eingangszeit
- Serviceziel
- Alter des Vorgangs
- vorhandene Abhängigkeiten
- benötigte Fähigkeiten
- zugesagte Termine
- Effizienz der gemeinsamen Bearbeitung

Ein älteres P3-Ticket sollte nicht dauerhaft durch neue P3-Tickets verdrängt werden.

Backlog-Steuerung sollte deshalb auch berücksichtigen:

- Ticketalter,
- blockierte Vorgänge,
- wiederholte Verschiebungen,
- und gefährdete Serviceziele.

Priorität darf nicht jede Planung zerstören

Hohe Prioritäten sollten tatsächlich besonderen Situationen vorbehalten bleiben.

Wenn sehr viele Vorgänge als P1 oder P2 eingestuft werden:

- verliert das Modell seine Aussagekraft,
- Ressourcen wechseln ständig,
- geplante Arbeit wird unterbrochen,
- Mitarbeiter werden überlastet,
- und wichtige Vorgänge konkurrieren miteinander.

Eine hohe Quote kritischer Prioritäten kann hinweisen auf:

- unklare Kriterien,
- unrealistische Serviceziele,
- falsche Benutzerwahl,
- organisatorische Fehlanreize,
- oder grundsätzlich instabile Services.

Prioritätsinflation

Prioritätsinflation entsteht, wenn immer mehr Vorgänge hoch priorisiert werden, um schneller bearbeitet zu werden.

Mögliche Anzeichen:

- Benutzer wählen regelmäßig „kritisch“.
- Führungskräfte verlangen Sonderbehandlung.
- Supportgruppen erhöhen Prioritäten zur Eskalation.
- Serviceziele werden nur durch formale Umklassifizierung eingehalten.
- fast jedes Ticket ist P1 oder P2.

Mögliche Maßnahmen:

- Kriterien präzisieren,
- Benutzerfelder überarbeiten,
- Priorität automatisch vorschlagen statt frei auswählen lassen,
- Stichproben durchführen,
- und Fehlanreize in Kennzahlen beseitigen.

Falsche Herabstufung

Prioritäten können ebenfalls zu niedrig angesetzt werden.

Mögliche Ursachen:

- geschäftlicher Kontext ist unbekannt,
- Benutzerzahl wird überbewertet,
- Sicherheitsauswirkung wird nicht erkannt,
- Servicekritikalität fehlt,
- oder Supportteam möchte Zielverletzungen vermeiden.

Beispiel:

Nur ein Benutzer meldet einen Fehler.

Dieser Benutzer ist jedoch für die gesetzlich fristgebundene Meldung verantwortlich.

Ohne Kontext könnte der Vorgang fälschlich als geringe Auswirkung bewertet werden.

Automatisierte Priorisierung

Werkzeuge können eine Priorität vorschlagen anhand von:

- ausgewähltem Service,
- Benutzerzahl,
- Standort,
- Incident-Art,
- Servicekritikalität,
- Monitoring-Daten,
- und bekannten Abhängigkeiten.

Vorteile:

- schnellere Ersterfassung,
- einheitlichere Bewertung,
- automatische Eskalation.

Risiken:

- unvollständige Eingangsdaten,
- veraltete Servicekritikalität,
- falsche Kategorien,
- unerkannte Ausnahmen,
- und zu starre Regeln.

> **Merke**
>
> Automatisierung kann Priorisierung unterstützen.
>
> Sie ersetzt nicht die fachliche Bewertung ungewöhnlicher Situationen.

KI-gestützte Priorisierung

KI kann Muster erkennen in:

- Tickettexten,
- betroffenen Services,
- vergangenen Incidents,
- Benutzerangaben,
- Monitoring-Daten,
- Kommunikationsverläufen.

Sie kann beispielsweise vorschlagen:

- mögliche Auswirkung,
- mögliche Dringlichkeit,
- Prioritätsstufe,
- notwendige Eskalation.

Mögliche Risiken:

- falsche Interpretation,
- Benachteiligung bestimmter Benutzergruppen,
- Überbewertung emotionaler Sprache,
- unerkannte Sicherheitsmeldungen,
- fehlende Nachvollziehbarkeit.

Notwendig sind:

- menschliche Überprüfung bei kritischen Fällen,
- transparente Kriterien,
- Qualitätsmessung,
- Korrekturmöglichkeiten,
- klare Ergebnisverantwortung.

Emotionale Sprache und KI

Eine KI darf nicht automatisch eine hohe Priorität setzen, nur weil ein Ticket Wörter enthält wie:

- dringend,
- sofort,
- katastrophal,
- Vorstand,
- kritisch.

Sie muss organisatorisch relevante Auswirkungen erkennen oder zur weiteren Klärung auffordern.

Beispiel:

> „Extrem dringend: Mauszeiger ist zu langsam.“

Die Formulierung allein beweist keine hohe Auswirkung oder Dringlichkeit.

Priorisierung bei Sicherheitsmeldungen

Eine Sicherheitsmeldung benötigt möglicherweise ein separates Bewertungsmodell.

Zusätzliche Kriterien können sein:

- Art des betroffenen Kontos
- Berechtigungsumfang
- aktive Ausnutzung
- Datenklassifizierung
- mögliche Ausbreitung
- Beweislage
- notwendige Meldefristen

Ein scheinbar kleiner Vorfall kann hohe Kritikalität besitzen.

Beispiel:

Nur ein Administratorkonto zeigt eine verdächtige Anmeldung.

Die Benutzerzahl ist gering.

Der mögliche Berechtigungsumfang ist jedoch sehr hoch.

Priorisierung bei Datenverlust

Zu klären sind:

- Welche Daten sind betroffen?
- Sind Sicherungen vorhanden?
- Werden weiterhin Daten überschrieben?
- Wie groß ist das Wiederherstellungsfenster?
- Sind rechtliche oder vertragliche Anforderungen betroffen?
- Kann die Datenquelle isoliert werden?
- Welche weiteren Benutzer oder Systeme sind gefährdet?

Die erste Priorität kann darin bestehen, weiteren Schaden zu verhindern.

Priorisierung bei Performance-Problemen

Ein Service kann technisch verfügbar sein, aber praktisch nicht ausreichend nutzbar.

Zu bewerten sind:

- tatsächliche Antwortzeiten,
- betroffene Benutzer,
- kritische Geschäftszeiten,
- Fehlerquote,

- mögliche Verschlechterung,
- verfügbare Alternativen.

Beispiel:

Eine Anwendung benötigt statt zwei Sekunden nun 30 Sekunden pro Vorgang.

Bei wenigen Vorgängen ist dies möglicherweise begrenzt.

Während eines Massenabrechnungslaufs kann dieselbe Verzögerung den gesamten Prozess blockieren.

Priorisierung bei geplanten Changes

Ein Incident nach einem Change kann besondere Aufmerksamkeit benötigen.

Zu prüfen sind:

- zeitlicher Zusammenhang,
- betroffene Services,
- Rückfallmöglichkeit,
- laufendes Wartungsfenster,
- Risiko weiterer Auswirkungen.

Die Priorität wird weiterhin anhand der tatsächlichen Auswirkung und Dringlichkeit bestimmt.

Ein Zusammenhang mit einem Change bedeutet nicht automatisch P1.

Priorisierung und Lieferanten

Bei Lieferantenfällen müssen möglicherweise zusätzlich berücksichtigt werden:

- Vertragsprioritäten
- Service-Level-Vereinbarungen
- Supportzeiten
- Eskalationswege
- Kundennummern
- notwendige Nachweise

Die interne Priorität und die Lieferantenpriorität können unterschiedliche Bezeichnungen besitzen.

Beispiel:

Intern:

> P1

Beim Provider:

> Severity 1

Die Organisation muss die Zuordnung kennen und prüfen, ob die Kriterien tatsächlich übereinstimmen.

Kommunikation einer Priorität

Benutzer müssen nicht zwingend jedes interne Prioritätsdetail verstehen.

Sie sollten jedoch nachvollziehen können:

- wie die Situation bewertet wurde,
- welcher nächste Schritt erfolgt,
- und wann sie eine Rückmeldung erhalten.

Geeignete Formulierung:

> Der Vorgang wurde als hohe Priorität eingestuft, weil der gesamte Standort betroffen ist und keine Zwischenlösung besteht. Das Netzwerkteam und der Provider arbeiten bereits an der Wiederherstellung. Die nächste Statusmeldung erfolgt spätestens um 10:30 Uhr.

Bei niedrigerer Priorität:

> Der Vorgang wird innerhalb der normalen Servicezeit bearbeitet. Aktuell ist ein Benutzer betroffen und ein alternativer Arbeitsplatz steht zur Verfügung. Sollte diese Alternative ausfallen, melden Sie sich bitte unter Angabe der Vorgangsnummer, damit die Priorität neu bewertet werden kann.

Keine Prioritätsdiskussion ohne Kontext

Ungeeignet:

>

> Das ist nur P3.

Besser:

> “ Nach den aktuellen Informationen ist eine Person betroffen und eine funktionsfähige Alternative vorhanden. Deshalb wird der Vorgang derzeit als P3 bearbeitet. Wenn weitere Benutzer betroffen sind oder die Alternative ausfällt, erhöhen wir die Priorität.

Governance der Priorisierung

Eine wirksame Priorisierung benötigt:

- dokumentierte Kriterien,
- klare Entscheidungsbefugnisse,
- nachvollziehbare Änderungen,
- geeignete Schulung,
- regelmäßige Qualitätsprüfung,
- Continual Improvement.

Zu klären ist:

- Wer definiert die Matrix?
- Wer genehmigt Änderungen?
- Wie werden kritische Services berücksichtigt?
- Wie werden Sicherheitsereignisse behandelt?
- Wie werden Zielzeiten festgelegt?
- Wie werden Fehlpriorisierungen erkannt?
- Welche Kennzahlen werden verwendet?
- Wie werden Ausnahmen entschieden?

Prioritätsmodell regelmäßig überprüfen

Das Modell kann ungeeignet werden durch:

- neue Services,
- veränderte Geschäftsprozesse,
- neue Standorte,
- organisatorische Veränderungen,
- neue Sicherheitsanforderungen,
- neue Servicezeiten.

Regelmäßig zu prüfen sind:

- Sind die Kriterien verständlich?
- Werden zu viele Tickets hoch priorisiert?
- Werden kritische Situationen zuverlässig erkannt?
- Passen Zielzeiten zu den Ressourcen?
- Werden Workarounds korrekt berücksichtigt?
- Sind Servicekritikalitäten aktuell?
- Gibt es wiederkehrende Ausnahmen?
- Unterstützt das Modell gewünschtes Verhalten?

Kennzahlen zur Priorisierung

Mögliche Kennzahlen:

- Anzahl der Tickets pro Prioritätsstufe
- Anteil nachträglich geänderter Prioritäten
- häufige Gründe für Erhöhungen
- häufige Gründe für Herabstufungen
- Zielerreichung je Priorität
- durchschnittliche Wiederherstellungszeit
- Anzahl falsch priorisierter Incidents
- Anzahl als kritisch gemeldeter, aber niedrig eingestufter Kontakte
- Wiedereröffnungsquote
- Benutzerbeschwerden über Priorisierung
- Anteil von Sicherheitsmeldungen mit korrekter Eskalation
- Alter des Backlogs je Priorität

Kennzahlen sollten nicht isoliert betrachtet werden.

Problematische Kennzahlen

Möglichst wenige P1-Incidents

Mögliche Fehlwirkung:

- kritische Incidents werden als P2 klassifiziert.

Möglichst hohe Zielerreichung

Mögliche Fehlwirkung:

- Prioritäten werden herabgesetzt,
- Zielzeiten werden gestoppt,
- Tickets werden voreilig geschlossen.

Möglichst kurze Lösungszeit

Mögliche Fehlwirkung:

- komplexe Ursachen werden nicht ausreichend dokumentiert,
- Workarounds werden als dauerhafte Lösung behandelt,
- Benutzerbestätigung wird übersprungen.

> **Merke**
>
> Kennzahlen dürfen nicht dazu führen, dass die Prioritätsbewertung manipuliert wird.

Praxisbeispiel: Ein Benutzer, hohe Auswirkung

Meldung

Ein einzelner Mitarbeiter kann eine Produktionsfreigabe nicht durchführen.

Zusätzlicher Kontext

- Nur dieses Konto besitzt aktuell die notwendige Freigabeberechtigung.
- Fertigungsaufträge warten.
- In 30 Minuten steht die Linie still.
- Kein geeigneter Stellvertreter ist verfügbar.

Bewertung

- Benutzerzahl: niedrig
- Auswirkung: hoch
- Dringlichkeit: hoch
- mögliche Priorität: P1

Das Beispiel zeigt, warum Benutzerzahl nicht allein ausreicht.

Praxisbeispiel: Viele Benutzer, niedrige Dringlichkeit

Meldung

Das interne Archivsystem ist für alle Benutzer nicht erreichbar.

Zusätzlicher Kontext

- Es wird für die aktuelle Tagesarbeit nicht benötigt.

- Am nächsten Arbeitstag findet eine Prüfung statt.
- Alle benötigten Unterlagen wurden vorübergehend exportiert.
- Es besteht kein Datenverlust.

Bewertung

- Benutzerkreis: groß
- Auswirkung: möglicherweise hoch
- unmittelbare Dringlichkeit: mittel oder niedrig
- mögliche Priorität: abhängig vom Organisationsmodell P2 oder P3

Praxisbeispiel: Führungskraft mit geringerer Auswirkung

Meldung

Eine Führungskraft kann einen zweiten Bildschirm nicht verwenden.

Zusätzlicher Kontext

- Hauptbildschirm funktioniert.
- alle Anwendungen sind nutzbar.
- kein zeitkritischer Termin wird beeinträchtigt.
- Ersatzgerät kann am nächsten Tag bereitgestellt werden.

Bewertung

- Auswirkung: niedrig
- Dringlichkeit: niedrig
- mögliche Priorität: P4

Die Position der meldenden Person verändert die technische Auswirkung nicht automatisch.

Praxisbeispiel: Aktive Sicherheitsbedrohung

Meldung

Ein einzelnes Administratorkonto zeigt mehrere ungewöhnliche Anmeldungen aus einem unbekannten Land.

Zusätzlicher Kontext

- Konto besitzt weitreichende Berechtigungen.
- eine Anmeldung war erfolgreich.
- Ursache ist noch unbekannt.

Bewertung

- Benutzerzahl: niedrig
- mögliche Sicherheitsauswirkung: sehr hoch
- Dringlichkeit: hoch
- sofortige Sicherheitseskalation erforderlich

Praxisbeispiel: Workaround reduziert Dringlichkeit

Meldung

Die Desktop-Version einer Fachanwendung startet nicht.

Zusätzlicher Kontext

- zehn Benutzer betroffen
- Webversion funktioniert vollständig
- Daten bleiben konsistent
- keine kritische Frist innerhalb der nächsten Stunden

Bewertung vor Workaround

- Auswirkung: mittel oder hoch
- Dringlichkeit: hoch

Bewertung nach bestätigtem Workaround

- Auswirkung weiterhin vorhanden
- unmittelbare Dringlichkeit möglicherweise geringer
- Priorität kann nach festgelegten Regeln neu bewertet werden

---

Praxisbeispiel: Priorität wird erhöht

Ursprüngliche Situation

Ein Benutzer kann keine Dateien speichern.

- ein Benutzer betroffen
- alternativer Ordner verfügbar
- Priorität P3

Neue Erkenntnis

Innerhalb von 20 Minuten melden weitere Benutzer dasselbe Problem.

Monitoring zeigt:

- zentraler Speicher fast vollständig belegt

- Schreibvorgänge schlagen für mehrere Services fehl
- Datenbankdienst könnte als Nächstes betroffen sein

Neue Bewertung

- Auswirkung: hoch
- Dringlichkeit: hoch
- Priorität wird auf P1 erhöht
- Incident-Koordination wird aktiviert

Praxisbeispiel: Request wird nicht zum Incident

Eine Führungskraft meldet am Freitagnachmittag:

> „Neuer Mitarbeiter beginnt Montag. Notebook, Konto und alle Anwendungen werden dringend benötigt.

Die Situation ist zeitkritisch.

Es handelt sich jedoch um eine verspätet eingereichte Onboarding-Anfrage und nicht automatisch um einen Incident.

Mögliche Behandlung:

- Request mit hoher interner Dringlichkeit erfassen
- Machbarkeit prüfen
- notwendige Genehmigungen und Risiken klären
- verfügbare Zwischenlösung anbieten
- Planungsproblem anschließend verbessern

Typische Fehler bei der Priorisierung

Fehler 1: Priorität nur nach Benutzerzahl bestimmen

Ein einzelner kritischer Arbeitsplatz wird unterschätzt.

Fehler 2: Priorität nach Hierarchie bestimmen

Führungskräfte erhalten automatisch P1.

Fehler 3: Benutzer bestimmt endgültige Priorität

Subjektive Dringlichkeit ersetzt organisatorische Kriterien.

Fehler 4: Jede Störung eines kritischen Service ist P1

Teilfunktionen und geeignete Workarounds werden nicht berücksichtigt.

Fehler 5: Technische Komplexität mit Priorität verwechseln

Schwierige Fehler werden bevorzugt, obwohl andere Vorgänge größere Auswirkungen besitzen.

Fehler 6: Priorität nach der Ersterfassung nie ändern

Ausbreitung und neue Risiken bleiben unberücksichtigt.

Fehler 7: Workaround automatisch als vollständige Lösung behandeln

Ursache und verbleibende Einschränkungen werden übersehen.

Fehler 8: Sicherheit nur nach Benutzerzahl bewerten

Ein kompromittiertes Administratorkonto wird unterschätzt.

Fehler 9: Zu viele P1- und P2-Tickets

Das Prioritätsmodell verliert seine Steuerungswirkung.

Fehler 10: Hohe Priorität zur Beschleunigung missbrauchen

Normale Requests verdrängen tatsächliche Incidents.

Fehler 11: Priorität senken, um Zielverletzung zu vermeiden

Kennzahlen werden manipuliert.

Fehler 12: Priorität und Major Incident gleichsetzen

Besondere Koordination wird entweder unnötig oder zu spät aktiviert.

Fehler 13: Zielzeit als Lösungsversprechen kommunizieren

Benutzer erhalten falsche Erwartungen.

Fehler 14: Zwischenlösung nicht fachlich prüfen

Unsichere oder unvollständige Alternativen führen zu falscher Herabstufung.

Fehler 15: Prioritätsänderung nicht dokumentieren

Spätere Entscheidungen sind nicht nachvollziehbar.

Fehler 16: Servicekritikalität ist veraltet

Neue geschäftliche Abhängigkeiten werden nicht erkannt.

Fehler 17: KI-Vorschlag ungeprüft übernehmen

Emotionale Sprache oder falsche Kategorien bestimmen die Priorität.

Bedeutung für Fachinformatiker für Systemintegration

Fachinformatiker liefern wichtige Informationen für die Prioritätsbewertung.

Sie können beurteilen:

- welcher Service betroffen ist,
- welche technischen Abhängigkeiten bestehen,
- wie weit sich ein Fehler ausbreitet,
- ob Datenverlust droht,
- ob ein Workaround technisch sicher ist,
- und welche weiteren Systeme gefährdet sind.

Technische Rückmeldungen sollten nicht nur lauten:

> Server ist ausgefallen.

Besser:

> Der Server unterstützt die zentrale Anmeldung für VPN und drei Cloud-Anwendungen. Aktuell können sich neue Benutzer nicht anmelden. Bestehende Sitzungen funktionieren noch. Ohne Wiederherstellung werden bei Ablauf der Sitzungen zunehmend weitere Benutzer betroffen sein. Ein sicherer Workaround besteht derzeit nicht.

Diese Informationen helfen bei der Bewertung von:

- Auswirkung,
- Dringlichkeit,
- Priorität,
- Eskalation.

30-Sekunden-Prüfung der Auswirkung

1. Welcher Service ist betroffen?
2. Welche Benutzer oder Kunden sind betroffen?
3. Welcher Geschäftsprozess ist beeinträchtigt?
4. Besteht vollständiger oder teilweiser Ausfall?
5. Gibt es Datenverlust oder Sicherheitsbezug?
6. Besteht eine geeignete Zwischenlösung?
7. Sind weitere Services abhängig?
8. Welche finanziellen, vertraglichen oder rechtlichen Folgen bestehen?
9. Besteht Gesundheits- oder Sicherheitsbezug?
10. Wie stark kann sich die Auswirkung noch vergrößern?

30-Sekunden-Prüfung der Dringlichkeit

1. Tritt der Schaden bereits ein?
2. Verschlimmert sich die Situation?
3. Wann wird ein kritischer Zeitpunkt erreicht?
4. Besteht eine zeitliche Frist?
5. Droht weiterer Datenverlust?
6. Besteht eine aktive Sicherheitsbedrohung?
7. Wie lange ist der Workaround nutzbar?
8. Kann die Bearbeitung sicher geplant werden?
9. Welche Wiederherstellungsfenster bestehen?
10. Wann müssen weitere Rollen oder Lieferanten eingebunden werden?

Checkliste für die Ersterfassung

- [ ] Ist der betroffene Service bekannt?
- [ ] Sind betroffene Benutzer, Standorte oder Kunden bekannt?
- [ ] Ist der betroffene Geschäftsprozess beschrieben?
- [ ] Ist der Umfang der Beeinträchtigung bekannt?
- [ ] Besteht vollständiger oder teilweiser Ausfall?
- [ ] Ist eine sichere Zwischenlösung vorhanden?
- [ ] Besteht möglicher Datenverlust?
- [ ] Besteht Sicherheits- oder Datenschutzbezug?
- [ ] Gibt es eine zeitkritische Frist?
- [ ] Wurde Auswirkung getrennt von Dringlichkeit bewertet?
- [ ] Ist die vorläufige Priorität begründet?
- [ ] Ist ein Zeitpunkt für die Neubewertung festgelegt?

Checkliste für hohe Priorität

- [ ] Sind die Kriterien für hohe Priorität tatsächlich erfüllt?
- [ ] Ist ein kritischer Service oder Geschäftsprozess betroffen?
- [ ] Besteht erheblicher Benutzer- oder Kundenbezug?
- [ ] Besteht keine ausreichende Zwischenlösung?
- [ ] Nimmt der Schaden weiter zu?
- [ ] Besteht Sicherheits-, Datenschutz- oder Datenverlustbezug?
- [ ] Sind notwendige Fachteams informiert?
- [ ] Ist Incident-Koordination erforderlich?
- [ ] Sind Lieferanten erreichbar und eingebunden?
- [ ] Ist die Kommunikationsverantwortung geklärt?
- [ ] Sind Statusintervalle festgelegt?
- [ ] Wird die Priorität regelmäßig neu bewertet?

Checkliste für eine Prioritätsänderung

- [ ] Welche neue Information liegt vor?
- [ ] Hat sich die Auswirkung verändert?
- [ ] Hat sich die Dringlichkeit verändert?
- [ ] Ist ein Workaround verfügbar oder ausgefallen?
- [ ] Sind weitere Benutzer oder Services betroffen?
- [ ] Ist ein neuer Sicherheits- oder Datenbezug entstanden?
- [ ] Wer hat die Änderung entschieden?
- [ ] Wurde der Grund dokumentiert?
- [ ] Wurden Eskalationen angepasst?
- [ ] Wurden Benutzer und Stakeholder informiert?
- [ ] Wurden Zielzeiten und Statusintervalle aktualisiert?

Checkliste für das Prioritätsmodell der Organisation

- [ ] Sind Auswirkung und Dringlichkeit eindeutig definiert?
- [ ] Sind die Bewertungsstufen verständlich?
- [ ] Sind kritische Services bekannt?
- [ ] Werden Sicherheits- und Datenschutzereignisse angemessen behandelt?
- [ ] Werden Gesundheits- und Sicherheitsrisiken berücksichtigt?
- [ ] Sind Prioritätsstufen eindeutig beschrieben?

- [ ] Sind Zielzeiten und Statusintervalle realistisch?
- [ ] Ist festgelegt, wer Prioritäten ändern darf?
- [ ] Sind Ausnahmen und Eskalationen geregelt?
- [ ] Werden Workarounds angemessen berücksichtigt?
- [ ] Werden Prioritätsänderungen dokumentiert?
- [ ] Werden Fehlpriorisierungen ausgewertet?
- [ ] Wird Prioritätsinflation überwacht?
- [ ] Wird das Modell regelmäßig verbessert?

Schnellreferenz

Frage	Zu bewertender Bereich
Wie viele Benutzer sind betroffen?	Auswirkung
Welcher Service ist betroffen?	Auswirkung
Welcher Geschäftsprozess steht still?	Auswirkung
Besteht Daten- oder Sicherheitsrisiko?	Auswirkung und Dringlichkeit
Gibt es einen geeigneten Workaround?	Auswirkung und Dringlichkeit
Wann verschlimmert sich die Situation?	Dringlichkeit
Welche Frist läuft ab?	Dringlichkeit
Wie schnell muss gehandelt werden?	Dringlichkeit
In welcher Reihenfolge wird bearbeitet?	Priorität
Welche Zielzeiten gelten?	Priorität und Service Level
Ist besondere Koordination notwendig?	Eskalation oder Major Incident
Muss die Bewertung geändert werden?	dynamische Neubewertung

Zusammenfassende Darstellung

> Incident oder Request wird erfasst
> ↓
> betroffenen Service und Geschäftsprozess bestimmen
> ↓
> Anzahl und Bedeutung der betroffenen Stakeholder bewerten
> ↓
> Daten-, Sicherheits-, Finanz- und Kundenfolgen berücksichtigen
> ↓

> **Auswirkung bestimmen**
> ↓
> Zeitdruck, Verschlechterung, Fristen und Workaround bewerten
> ↓
> **Dringlichkeit bestimmen**
> ↓
> organisatorische Matrix oder Entscheidungsregel anwenden
> ↓
> **Priorität festlegen und begründen**
> ↓
> Zielzeiten, Ownership, Eskalation und Kommunikation auslösen
> ↓
> Situation fortlaufend beobachten
> ↓
> Priorität bei neuen Erkenntnissen erhöhen oder senken
> ↓
> Entscheidung und Auswirkungen nachvollziehbar dokumentieren

---

Verwandte Seiten

- 3.1 Der Service Desk als zentraler Kontaktpunkt
- 3.2 Kontaktkanäle und Erreichbarkeit
- 3.3 Benutzerkommunikation und professioneller Umgang
- 3.4 Tickets vollständig erfassen und kategorisieren
- 3.6 Erstdiagnose, Lösung und funktionale Eskalation
- 3.7 Ownership, hierarchische Eskalation und Major Incidents
- 3.8 Self-Service, Wissensnutzung und Automatisierung
- 3.9 Kennzahlen, Qualität und Continual Improvement im Service Desk
- Incident Management
- Service Request Management
- Information Security Management
- Service Level Management
- Service Continuity Management
- Measurement and Reporting

Quellen und Versionsstand

Offizielle Grundlagen

- PeopleCert: ITIL 4 Practitioner – Incident Management
- PeopleCert: ITIL 4 Practitioner – Service Desk
- ITIL: ITIL Service – Version 5

- PeopleCert: ITIL Foundation – Version 5

Offiziell bestätigter Stand

Die offiziellen ITIL- und PeopleCert-Quellen bestätigen:

- Incident Management dient der schnellen Wiederherstellung des normalen Servicebetriebs nach Störungen.
- Incident Management umfasst Prozesse, Rollen, Informationen, Technologien, Partner, Messgrößen und die Integration in organisatorische Wertströme.
- Einheitliche Arbeitsweisen und ein gemeinsames Verständnis helfen, inkonsistente Priorisierung und übersehene wichtige Vorgänge zu vermeiden.
- Service-Desk- und Incident-Management-Practices müssen an organisatorische Bedürfnisse, Wertströme und Services angepasst werden.
- ITIL Version 5 führt die Management Practices fort und richtet digitale Servicearbeit an Outcomes, Erfahrung, Resilienz und Ende-zu-Ende-Zusammenarbeit aus.

Einordnung

Die auf dieser Seite dargestellten:

- Auswirkungs- und Dringlichkeitsstufen,
- Prioritätsmatrix,
- P1-bis-P4-Bezeichnungen,
- Zielzeitbeispiele,
- Statusintervalle,
- Entscheidungskriterien,
- Praxisbeispiele,
- und Checklisten

sind herstellerneutrale redaktionelle Praxisempfehlungen dieses unabhängigen Nachschlagewerks.

ITIL schreibt keine universelle:

- Prioritätsmatrix,
- Anzahl von Prioritätsstufen,
- Reaktionszeit,
- Wiederherstellungszeit,
- Severity-Skala,
- VIP-Regel,
- oder Major-Incident-Grenze

für alle Organisationen vor.

Die konkrete Gestaltung muss angepasst werden an:

- Produkte und Services,

- Geschäftsprozesse,
- Servicekritikalität,
- Benutzer und Kunden,
- Sicherheits- und Datenschutzanforderungen,
- gesetzliche Verpflichtungen,
- Servicezeiten,
- Fähigkeiten,
- Lieferanten,
- verfügbare Ressourcen.

Behandelter Framework-Stand: ITIL Version 5
Zusätzlich berücksichtigt: aktuelle öffentlich zugängliche ITIL-4-Practice-Guidance
Fachlicher Stand: August 2026
