

3.2 Kontaktkanäle und Erreichbarkeit

“ Kurz erklärt

Kontaktkanäle bestimmen, wie Benutzer den Service Desk erreichen können.

Typische Kanäle sind:

- Self-Service-Portal,
- Telefon,
- E-Mail,
- Chat,
- virtueller Agent,
- mobile Anwendung,
- persönlicher Vor-Ort-Kontakt,
- und besonders definierte Meldewege für Notfälle oder Sicherheitsereignisse.

Erreichbarkeit beschreibt mehr als die technische Verfügbarkeit eines Kanals.

Ein Kanal ist erst dann wirksam, wenn:

- Benutzer ihn kennen,
- er für das jeweilige Anliegen geeignet ist,
- er zuverlässig überwacht wird,
- eine Bearbeitung innerhalb angemessener Zeiten erfolgt,
- Informationen nicht verloren gehen,
- und bei Bedarf ein Wechsel zu menschlicher Unterstützung möglich ist.

ITIL schreibt keine universelle Anzahl von Kanälen und keinen grundsätzlich rund um die Uhr besetzten Service Desk vor.

Die Organisation gestaltet Kanäle, Servicezeiten und Eskalationswege entsprechend ihren Benutzern, Services, Risiken und verfügbaren Fähigkeiten.

Warum die Gestaltung der Kontaktkanäle wichtig ist

Ein Service Desk kann fachlich gut organisiert sein und trotzdem schlecht erreichbar wirken.

Beispiele:

- Das Portal ist vorhanden, aber Benutzer finden das passende Formular nicht.
- Die Support-E-Mail-Adresse wird nur unregelmäßig geprüft.

- Der Chat zeigt „verfügbar“, obwohl kein Mitarbeiter angemeldet ist.
- Eine Telefonnummer ist veröffentlicht, aber außerhalb der Servicezeit gibt es keine verständliche Ansage.
- Ein virtueller Agent beantwortet Standardfragen, bietet jedoch keinen Übergang zu einem Menschen.
- Benutzer melden kritische Störungen über einen Kanal, der erst am nächsten Arbeitstag bearbeitet wird.
- Mehrere Kontaktkanäle erzeugen voneinander unabhängige Tickets für dasselbe Anliegen.
- Eine Sicherheitsmeldung wird in einem allgemeinen Supportkanal mit ungeeigneten Zugriffsrechten erfasst.

Die Wahl und Gestaltung der Kontaktkanäle beeinflusst damit:

- Erfassungsqualität,
- Bearbeitungsgeschwindigkeit,
- Benutzeraufwand,
- Informationssicherheit,
- Barrierefreiheit,
- Priorisierung,
- Kommunikation,
- Nachvollziehbarkeit,
- und die gesamte Benutzererfahrung.

“ Merke

Viele Kontaktkanäle bedeuten nicht automatisch gute Erreichbarkeit.

Jeder angebotene Kanal muss zuverlässig betrieben, überwacht und in die gemeinsamen Wertströme eingebunden werden.

Kontaktkanal, Servicezeit und Reaktionszeit unterscheiden

Begriff	Bedeutung
Kontaktkanal	Weg, über den ein Benutzer mit dem Service Provider in Verbindung tritt
technische Verfügbarkeit	Zeitraum, in dem der Kanal technisch erreichbar ist
Servicezeit	Zeitraum, in dem eine vereinbarte menschliche oder automatisierte Leistung angeboten wird
Supportzeit	Zeitraum, in dem Unterstützung für einen bestimmten Service bereitsteht
Betriebszeit	Zeitraum, in dem ein Produkt oder Service regulär genutzt werden soll

Begriff	Bedeutung
Bereitschaftszeit	Zeitraum, in dem zuständige Personen außerhalb regulärer Zeiten bei bestimmten Ereignissen reagieren
erste Reaktionszeit	Zeit bis zu einer ersten qualifizierten Rückmeldung
Bearbeitungszeit	Zeit, in der aktiv an einem Anliegen gearbeitet wird
Lösungs- oder Erfüllungszeit	Zeit bis zur ausreichenden Wiederherstellung oder Erfüllung
Statusintervall	vereinbarter Abstand zwischen Statusinformationen

Diese Zeiten können unterschiedlich sein.

Beispiel:

- Ein Portal ist technisch 24 Stunden täglich erreichbar.
- Neue Standardanfragen werden nur montags bis freitags bearbeitet.
- Kritische Incidents können außerhalb dieser Zeit über eine Bereitschaftsnummer gemeldet werden.
- Ein bestimmter Produktionsservice wird rund um die Uhr betrieben.
- Nichtkritische Fragen zu diesem Service werden trotzdem nur während der normalen Service-Desk-Zeit beantwortet.

“ Wichtig

Ein technisch rund um die Uhr erreichbares Formular bedeutet nicht automatisch einen rund um die Uhr verfügbaren menschlichen Support.

Die Kanalstrategie am Benutzerbedarf ausrichten

Vor der Einführung oder Änderung von Kontaktkanälen sollte die Organisation untersuchen:

- Welche Benutzergruppen werden unterstützt?
- Wo und wann arbeiten diese Benutzer?
- Welche Geräte stehen ihnen zur Verfügung?
- Welche Sprachen werden benötigt?
- Welche technischen Fähigkeiten können vorausgesetzt werden?
- Welche Services sind besonders kritisch?
- Welche Anliegen treten häufig auf?
- Welche Situationen benötigen sofortige menschliche Kommunikation?
- Welche Anliegen lassen sich sicher standardisieren?
- Welche gesetzlichen, vertraglichen oder betrieblichen Anforderungen gelten?
- Welche Barrieren können Benutzer vom Kontakt abhalten?
- Welche Kanäle können zuverlässig betrieben werden?

Unterschiedliche Benutzergruppen können unterschiedliche Anforderungen besitzen.

Beispiele:

Benutzergruppe	Mögliche Anforderungen
Büroarbeitsplätze	Portal, E-Mail, Chat und Telefon
Produktionsmitarbeiter	leicht erreichbare Telefonnummer oder lokaler Kontakt
Außendienst	mobile Erreichbarkeit und Self-Service
Schichtbetrieb	erweiterte Support- oder Bereitschaftszeiten
externe Kunden	klar getrenntes Kundenportal und vertraglich definierte Kanäle
Führungskräfte	dieselben Prioritätsregeln, aber möglicherweise besondere Kommunikationsanforderungen
Benutzer mit Einschränkungen	barrierearme Kanäle und alternative Kontaktmöglichkeiten
internationale Benutzer	unterschiedliche Zeitzonen und Sprachen
Administratoren	technischer Eskalations- und Sicherheitskanal

“ Grundsatz

Der bevorzugte Kanal der IT ist nicht automatisch der geeignete Kanal für alle Benutzer.

Single Point of Contact und mehrere Kanäle

Der Service Desk wird häufig als zentraler oder einzelner Kontaktpunkt beschrieben.

Das bedeutet nicht zwingend, dass nur ein einziger Kanal erlaubt ist.

Mehrere Kanäle können gemeinsam einen zentralen Kontaktpunkt bilden, wenn sie:

- eindeutig zum selben Service Desk führen,
- gemeinsame Informationen verwenden,
- Kontakte nachvollziehbar zusammenführen,
- einheitliche Prioritäts- und Eskalationsregeln anwenden,
- und konsistente Statusinformationen liefern.

Beispiel:

Ein Benutzer kann den Service Desk erreichen über:

- Portal,
- Telefon,
- E-Mail,
- oder Chat.

Alle Kontakte werden jedoch:

- im selben Vorgangssystem dokumentiert,
- auf mögliche Duplikate geprüft,
- nach denselben Kriterien eingeordnet,
- und mit einer gemeinsamen Statussicht bearbeitet.

Problematisch wäre dagegen:

- Portal-Tickets werden vom Service Desk bearbeitet.
- E-Mails landen bei einzelnen Administratoren.
- Chatkontakte werden nicht dokumentiert.
- Telefonmeldungen befinden sich in privaten Notizen.
- Vor-Ort-Anfragen werden gar nicht erfasst.

“Merke

Ein zentraler Kontaktpunkt ist eine organisatorische Fähigkeit und nicht nur eine einzelne Telefonnummer oder E-Mail-Adresse.

Mehrkanal und kanalübergreifende Bearbeitung

Eine Organisation kann mehrere Kanäle anbieten.

Dabei sollte unterschieden werden zwischen:

Ansatz	Bedeutung
Mehrkanalbetrieb	mehrere Kanäle existieren nebeneinander
kanalübergreifende Bearbeitung	Informationen und Bearbeitungsstand bleiben beim Kanalwechsel erhalten
einheitliche Serviceerfahrung	Regeln, Sprache und Statusinformationen sind über die Kanäle hinweg abgestimmt

Beispiel einer schlechten kanalübergreifenden Erfahrung:

1. Benutzer meldet eine Störung per Chat.
2. Der Chat verweist auf eine Telefonnummer.
3. Am Telefon muss der Benutzer alles erneut erklären.

4. Später erhält er eine E-Mail mit einer neuen Ticketnummer.
5. Im Portal ist keiner der bisherigen Schritte sichtbar.

Bessere Gestaltung:

1. Chat erfasst die ersten Informationen.
2. Ein Vorgang wird erstellt.
3. Beim Wechsel zum Telefon sieht der Mitarbeiter den bisherigen Verlauf.
4. Der Benutzer nennt nur noch die Vorgangsnummer oder wird sicher identifiziert.
5. Status und Ergebnis bleiben im Portal sichtbar.

Die konkrete technische Umsetzung hängt von den verwendeten Werkzeugen ab.

Kanalwahl nach Art des Anliegens

Nicht jeder Kanal ist für jedes Anliegen gleich geeignet.

Anliegen	Häufig geeignete Kanäle
standardisierte Softwareanforderung	Self-Service-Portal
planbarer Berechtigungsantrag	Portal mit strukturiertem Formular
allgemeine Frage	Portal, Knowledge-Base, Chat oder E-Mail
komplexe Störung mit Rückfragen	Telefon, Chat oder persönlicher Kontakt
kritischer Serviceausfall	definierter dringender Meldeweg
möglicher Sicherheitsvorfall	besonderer Sicherheitsmeldeweg
Kennwort vergessen	sicherer Self-Service oder verifizierter Supportkontakt
Statusabfrage	Portal oder automatische Benachrichtigung
Feedback oder Beschwerde	Portal, Umfrage, E-Mail oder persönlicher Kontakt
Ausfall des normalen Portals	alternativer Kontaktweg

Die Organisation sollte deutlich kommunizieren:

- welche Kanäle existieren,
- wofür sie gedacht sind,
- wann sie bearbeitet werden,
- und welcher Kanal bei dringenden Situationen verwendet werden muss.

Das Self-Service-Portal

Ein Self-Service-Portal kann Benutzer dabei unterstützen:

- Incidents zu melden,

- Service Requests auszuwählen,
- Wissen zu durchsuchen,
- Statusinformationen einzusehen,
- Genehmigungen abzugeben,
- Rückfragen zu beantworten,
- und standardisierte Leistungen selbst auszuführen.

Mögliche Vorteile:

- strukturiertere Informationen,
- rund um die Uhr mögliche Erfassung,
- transparente Statussicht,
- weniger Medienbrüche,
- automatische Weiterleitung,
- und Unterstützung standardisierter Wertströme.

Mögliche Nachteile bei schlechter Gestaltung:

- unverständliche Kategorien,
- zu viele Formulare,
- lange Pflichtfeldlisten,
- technische Begriffe,
- schlechte Suchfunktion,
- fehlende mobile Nutzbarkeit,
- kein erkennbarer Kontakt zu einem Menschen,
- und hohe Abbruchquoten.

“ Merke

Ein Portal ist kein Selbstzweck.

Es muss den Benutzeraufwand reduzieren und die Bearbeitung verbessern.

Ein verständliches Portal gestalten

Ein Benutzer sollte möglichst nicht wissen müssen:

- welches technische Team zuständig ist,
- welche Datenbank betroffen sein könnte,
- welche Practice verwendet wird,
- oder welche interne Komponentenkategorie ausgewählt werden muss.

Ungeeignete Auswahl:

- Active Directory
- Entra ID
- LDAP
- SAML
- OIDC
- RADIUS
- PKI

Verständlichere Auswahl:

- Ich kann mich nicht anmelden.
- Mein Konto ist gesperrt.
- Die Mehrfaktor-Anmeldung funktioniert nicht.
- Ich benötige einen neuen Zugriff.
- Ich möchte ein Kennwort ändern.
- Ich vermute einen unberechtigten Zugriff.

Die technische Zuordnung kann anschließend:

- durch Regeln,
- durch den Service Desk,
- oder durch geeignete Automatisierung

erfolgen.

Formulare zweckmäßig gestalten

Ein Portalformular sollte nur Informationen verlangen, die für:

- Einordnung,
- Entscheidung,
- Bearbeitung,
- Kontrolle,
- oder spätere Auswertung

benötigt werden.

Mögliche Gestaltungsmittel:

- einfache Sprache,
- kurze Hilfetexte,
- Beispiele,
- dynamisch eingeblendete Felder,
- sinnvolle Standardwerte,
- automatische Übernahme bekannter Benutzerdaten,
- Auswahl verständlicher Services,

- und sichtbare Angabe der erwarteten Bearbeitungszeit.

Ungeeignete Pflichtfelder:

- interne Supportgruppe,
- vermutete technische Ursache,
- interne CI-Kennung,
- oder eine Priorität, deren Kriterien der Benutzer nicht kennt.

Besser:

- betroffener Service,
- beobachtetes Symptom,
- betroffene Personen oder Standorte,
- benötigter Zeitpunkt,
- und mögliche Auswirkungen.

Portal und Barrierefreiheit

Ein Portal sollte von möglichst vielen Benutzern selbstständig verwendet werden können.

Zu berücksichtigen sind beispielsweise:

- Tastaturbedienbarkeit,
- verständliche Beschriftungen,
- ausreichende Kontraste,
- skalierbare Darstellung,
- kompatible Formulare,
- verständliche Fehlermeldungen,
- keine ausschließliche Informationsvermittlung über Farbe,
- alternative Texte für relevante grafische Inhalte,
- und alternative Kontaktmöglichkeiten.

Die konkreten verbindlichen Anforderungen hängen von Organisation, Land, Branche und Zielgruppe ab.

“ Wichtig

Wenn ein Portal für einen Benutzer nicht nutzbar ist, muss ein angemessener alternativer Kontaktweg bestehen.

Telefonischer Kontakt

Telefon eignet sich besonders für:

- dringende Situationen,
- komplexe Fehlerbilder,
- emotional belastende Incidents,
- Rückfragen in Echtzeit,
- und Benutzer, die keinen Zugang zum Portal besitzen.

Mögliche Vorteile:

- unmittelbare Interaktion,
- schnelle Klärung,
- bessere Wahrnehmung von Unsicherheit oder Dringlichkeit,
- und direkte Anleitung.

Mögliche Herausforderungen:

- Wartezeiten,
- eingeschränkte Nachvollziehbarkeit ohne Dokumentation,
- Missverständnisse,
- Sprachprobleme,
- hoher Personalbedarf,
- und fehlende Übertragung technischer Details.

Der Service Desk sollte deshalb sicherstellen:

- verständliche Begrüßung,
- notwendige Identitätsprüfung,
- strukturierte Erfassung,
- Dokumentation während oder unmittelbar nach dem Gespräch,
- realistische Statusaussagen,
- und eindeutige nächste Schritte.

Telefonmenü und Warteschlange

Ein Telefonmenü kann Kontakte vorsortieren.

Es sollte jedoch:

- möglichst kurz,
- verständlich,
- aktuell,
- und auf tatsächlich unterschiedliche Bearbeitungswege beschränkt

sein.

Ungeeignet:

“ Drücken Sie 1 für Incident Management, 2 für Service Request Management, 3 für Configuration Management.

Benutzer kennen diese internen Begriffe möglicherweise nicht.

Verständlicher:

“ Drücken Sie 1 bei einer aktuellen technischen Störung.
Drücken Sie 2 für eine Bestellung oder Zugriffsanfrage.
Drücken Sie 3 bei einer verdächtigen E-Mail oder einem möglichen Sicherheitsvorfall.

Bei Warteschlangen können hilfreich sein:

- ungefähre Warteinformation,
- Rückrufmöglichkeit,
- Hinweis auf geeigneten Self-Service,
- und verständliche Ansage für dringende Notfälle.

E-Mail als Kontaktkanal

E-Mail ist leicht zugänglich und eignet sich unter anderem für:

- weniger dringende Anliegen,
- schriftliche Rückfragen,
- Übermittlung strukturierter Informationen,
- und Kommunikation mit externen Partnern.

Mögliche Nachteile:

- unvollständige Angaben,
- uneindeutige Betreffzeilen,
- lange E-Mail-Verläufe,
- unkontrollierte Anhänge,
- fehlende Prioritätsinformationen,
- Duplikate,
- und Sicherheitsrisiken.

Eine Support-E-Mail-Adresse sollte möglichst:

- automatisch eine Eingangsbestätigung senden,
- eine Vorgangsnummer erzeugen,
- keine privaten Postfächer verwenden,
- regelmäßig überwacht werden,
- und klare Hinweise zu Servicezeiten enthalten.

“ Sicherheitsrelevant

E-Mail ist nicht für jede vertrauliche Information oder jeden Sicherheitsvorfall geeignet.

Die Organisation muss zulässige Inhalte und alternative sichere Übertragungswege festlegen.

Gute Betreffzeilen und E-Mail-Inhalte

Ungeeigneter Betreff:

“ Hilfe!!!

Besser:

“ Anmeldung am Zeiterfassungssystem nicht möglich – Standort Mitte

Hilfreiche Angaben:

- betroffener Benutzer,
- betroffener Service,
- beobachtetes Verhalten,
- Fehlermeldung,
- Beginn,
- Auswirkung,
- bereits durchgeführte Schritte,
- und sichere Kontaktmöglichkeit.

Der Service Desk sollte Benutzer nicht mit langen technischen Vorlagen überfordern.

Kurze Hinweise oder automatische Fragen können die Qualität verbessern.

Chat und Instant Messaging

Chat eignet sich für:

- kurze Rückfragen,
- schnelle Orientierung,
- begleitete Diagnose,
- und weniger formelle Kommunikation.

Mögliche Vorteile:

- direkte schriftliche Kommunikation,
- Übertragung kurzer technischer Informationen,
- geringer Wechsel zwischen Arbeit und Support,
- und parallele Bearbeitung mehrerer Kontakte.

Mögliche Risiken:

- unvollständige Dokumentation,
- private Chats außerhalb des Supportsystems,
- Erwartung sofortiger Antwort,
- Übermittlung sensibler Inhalte,
- und Verlust des Verlaufs.

Geeignete Regeln:

- offizieller Service-Desk-Chat statt privater Direktnachrichten,
- Übernahme relevanter Informationen in den Vorgang,
- klare Anzeige der Servicezeit,
- sichere Identitätsprüfung bei kritischen Aktionen,
- und Möglichkeit zur Eskalation an einen Menschen oder einen anderen Kanal.

Privatnachrichten an Administratoren

Direkte Nachrichten an bekannte Administratoren wirken für Benutzer häufig schnell.

Sie erzeugen jedoch mögliche Probleme:

- keine zentrale Übersicht,
- unklare Priorisierung,
- fehlende Vertretung,
- Unterbrechung konzentrierter Arbeit,
- keine dokumentierte Kommunikation,
- und Abhängigkeit von einzelnen Personen.

Eine professionelle Reaktion kann lauten:



Ich unterstütze gern. Bitte sende die Meldung über den Service-Desk-Kanal oder erlaube mir, daraus einen Vorgang zu erstellen. Dadurch bleibt die Bearbeitung auch bei meiner Abwesenheit nachvollziehbar.

Bei kritischen Situationen sollte die Meldung nicht nur zurückgewiesen werden.

Der Mitarbeiter sollte sicherstellen, dass:

- der Vorgang erfasst,
- richtig eskaliert,
- und nicht durch die formale Kanalregel verzögert

wird.

Virtuelle Agenten und Chatbots

Ein virtueller Agent kann Benutzer unterstützen bei:

- häufigen Fragen,
- Statusabfragen,
- Auswahl eines Serviceangebots,
- Erfassung strukturierter Angaben,
- sicheren standardisierten Selbsthilfesritten,
- und Weiterleitung an einen Menschen.

Mögliche Vorteile:

- unmittelbare Unterstützung,
- hohe Skalierbarkeit,
- längere Erreichbarkeit,
- und Entlastung bei wiederkehrenden Anliegen.

Mögliche Risiken:

- falsche Interpretation,
- unpassende Antworten,
- Schleifen ohne Lösung,
- fehlende Transparenz,
- unzureichende Barrierefreiheit,
- und fehlender menschlicher Eskalationsweg.

„ Grundsatz

Ein virtueller Agent sollte nicht vorgeben, ein Mensch zu sein.

Benutzer sollten erkennen können, dass sie mit einem automatisierten System interagieren.

Menschliche Übergabe bei virtuellen Agenten

Ein Übergang zu einem Mitarbeiter sollte insbesondere möglich sein, wenn:

- die Anfrage nicht verstanden wird,
- mehrere Lösungsversuche scheitern,
- die Situation kritisch ist,
- Sicherheits- oder Datenschutzbezug besteht,
- der Benutzer ausdrücklich menschliche Unterstützung benötigt,
- oder der virtuelle Agent keine ausreichende Befugnis besitzt.

Bei der Übergabe sollten bereits erfasste Informationen erhalten bleiben.

Ungeeignet:

1. Benutzer beantwortet zehn Fragen im Chatbot.
2. Der Chatbot bietet eine Telefonnummer an.
3. Der Mitarbeiter sieht keine bisherigen Angaben.
4. Der Benutzer beginnt erneut.

Besser:

1. Virtueller Agent erfasst grundlegende Angaben.
2. Ein Vorgang wird erzeugt.
3. Der Mitarbeiter erhält Verlauf und bisherige Ergebnisse.
4. Der Benutzer wird über die Übergabe informiert.

Mobile Anwendungen

Eine mobile Supportanwendung kann hilfreich sein für:

- Außendienst,
- mobile Mitarbeiter,
- Produktionsumgebungen,
- Push-Benachrichtigungen,
- Statusabfragen,
- und Erfassung von Fotos oder Gerätecodes.

Zu berücksichtigen sind:

- Authentifizierung,
- Geräteverwaltung,
- Datenschutz,
- sichere Speicherung,
- Offline-Verhalten,
- Bedienbarkeit,
- und Möglichkeit eines alternativen Kontaktwegs.

Fotos und Anhänge sollten nur erfasst werden, wenn sie notwendig sind.

Dabei können versehentlich sichtbar werden:

- personenbezogene Daten,
- Bildschirminhalte,
- Zugangsinformationen,
- Produktionsinformationen,
- oder vertrauliche Dokumente.

Persönlicher Vor-Ort-Kontakt

Ein persönlicher Kontakt kann sinnvoll sein bei:

- Hardwareproblemen,
- komplexen Benutzerfragen,
- Einarbeitung,
- Arbeitsplätzen ohne digitalen Zugang,
- und Situationen, in denen Beobachtung des tatsächlichen Arbeitsumfelds wichtig ist.

Mögliche Modelle:

- Walk-up Desk,
- lokale Supportzeiten,
- IT-Sprechstunde,
- Terminvereinbarung,
- oder gezielter Vor-Ort-Einsatz.

Auch ein persönlicher Kontakt sollte nachvollziehbar dokumentiert werden, wenn:

- eine Bearbeitung,
- ein Asset-Wechsel,
- eine Sicherheitsentscheidung,
- ein Incident,
- oder eine weitere Maßnahme

entsteht.



Typischer Fehler

Vor-Ort-Hilfe wird vollständig außerhalb des Service-Management-Systems durchgeführt.

Dadurch bleiben Aufwand, wiederkehrende Probleme und wichtige Änderungen unsichtbar.

Walk-up Desk

Ein Walk-up Desk ist ein physischer Kontaktpunkt, an dem Benutzer persönlich Unterstützung erhalten.

Mögliche Vorteile:

- unmittelbare menschliche Hilfe,
- gute Unterstützung bei Geräten,
- geringe Hürde,
- und bessere Wahrnehmung des Benutzerkontexts.

Mögliche Herausforderungen:

- Warteschlangen,
- Unterbrechungen,
- unklare Priorisierung,
- nicht dokumentierte Tätigkeiten,
- und Benutzer aus anderen Standorten werden benachteiligt.

Zu klären sind:

- Öffnungszeiten,
- geeignete Anliegen,
- Termin- oder Warteschlangenmodell,
- Identitätsprüfung,
- Umgang mit Geräten,
- Dokumentation,
- und Eskalation.

Automatisch erzeugte Kontakte

Nicht jeder Kontakt wird durch einen Menschen ausgelöst.

Mögliche technische Quellen:

- Monitoring,
- Event-Management-System,
- Endgeräteverwaltung,
- Sicherheitsplattform,
- Backup-System,
- Cloud-Provider,
- oder Integrationsschnittstelle.

Solche Meldungen können automatisch:

- ein Ticket,
- ein Event,
- einen Incident,
- oder eine andere Arbeitsaufgabe

erzeugen.

Dabei muss geklärt sein:

- Welche technische Meldung benötigt tatsächlich eine Handlung?
- Wird bereits ein Vorgang bearbeitet?
- Welche Priorität ist angemessen?
- Wer besitzt die Verantwortung?
- Wie werden Duplikate verhindert?
- Wann müssen Benutzer informiert werden?

“ **Merke**

Eine automatische Meldung ist nicht automatisch ein Incident.

Sie muss entsprechend ihrer Bedeutung und Auswirkung eingeordnet werden.

Besondere Meldewege für Sicherheitsereignisse

Mögliche Sicherheitsereignisse benötigen häufig einen besonders definierten Meldeweg.

Beispiele:

- verdächtige E-Mail,
- verlorenes Gerät,
- möglicher unberechtigter Zugriff,
- Schadsoftware,
- versehentliche Datenoffenlegung,
- oder verdächtiger Anruf.

Der Meldeweg sollte:

- leicht auffindbar,
- schnell erreichbar,
- sicher,
- und den Benutzern bekannt

sein.

Zusätzlich ist festzulegen:

- welche Informationen erfasst werden,
- wer Zugriff auf die Meldung erhält,
- wann das Sicherheitsteam eingebunden wird,
- welche Kommunikation verwendet werden darf,
- und wie Beweise geschützt werden.

Ungeeignet wäre ein verstecktes Formular mit vielen technischen Pflichtfeldern.

Notfall- und Major-Incident-Kanäle

Für besonders kritische Incidents kann ein eigener dringender Meldeweg sinnvoll sein.

Dieser darf nicht zur allgemeinen Beschleunigung normaler Anliegen missbraucht werden.

Mögliche Regeln:

- Welche Kriterien rechtfertigen den Kanal?
- Wer darf ihn verwenden?
- Welche Services sind umfasst?
- Welche Informationen müssen genannt werden?
- Wer nimmt die Meldung entgegen?
- Wie wird der Major-Incident-Prozess aktiviert?
- Wie wird die Kommunikation koordiniert?
- Was geschieht bei Fehllarm?

Beispiel:

Ein Portalhinweis kann lauten:

“ Bei vollständigem Ausfall eines kritischen Produktionsservice außerhalb der Service-Desk-Zeit verwenden Sie die Bereitschaftsnummer. Normale Bestellungen und Einzelplatzprobleme werden am nächsten Arbeitstag bearbeitet.

Alternative Kanäle bei Ausfall des Service Desk

Der normale Kontaktweg kann selbst ausfallen.

Beispiele:

- Ticketsystem nicht erreichbar,
- E-Mail-Service gestört,
- Telefonanlage ausgefallen,
- Identitätsdienst verhindert Portalzugriff,
- oder Standortverbindung unterbrochen.

Deshalb sollte ein alternativer Meldeweg vorbereitet sein.

Mögliche Alternativen:

- externe Statusseite,
- separate Notfallnummer,
- unabhängige Mobilfunknummer,
- alternativer Kommunikationsdienst,
- definierter lokaler Ansprechpartner,
- oder Providerkontakt.

Der alternative Kanal sollte nicht von derselben ausgefallenen Komponente abhängen.

“ Praxistipp

Die Notfallkontaktinformationen sollten auch verfügbar sein, wenn das interne Netzwerk, das Portal oder das Identitätssystem nicht funktioniert.

Statusseite

Eine Statusseite kann Benutzer über bekannte Störungen, Wartungen und Wiederherstellungen informieren.

Mögliche Inhalte:

- betroffener Service,
- Beginn,
- bekannte Auswirkung,
- aktueller Status,
- Zwischenlösung,
- nächstes Update,

- und Abschlussinformation.

Vorteile:

- weniger Mehrfachmeldungen,
- konsistente Kommunikation,
- geringerer Benutzeraufwand,
- und Entlastung des Service Desk.

Zu berücksichtigen sind:

- Zielgruppe,
- Zugriffsrechte,
- vertrauliche Informationen,
- Verantwortlichkeit für Aktualisierungen,
- und technische Unabhängigkeit von betroffenen Services.

Eine externe Statusseite darf keine sicherheitskritischen internen Details offenlegen.

Servicezeiten bestimmen

Servicezeiten sollten sich an den benötigten Outcomes und Risiken orientieren.

Zu untersuchen sind:

- Betriebszeiten wichtiger Services,
- Arbeitszeiten der Benutzer,
- internationale Zeitzonen,
- Schichtbetrieb,
- vertragliche Vereinbarungen,
- saisonale Spitzen,
- Sicherheitsanforderungen,
- und verfügbare Bereitschaft.

Mögliche Modelle:

- normale Geschäftszeiten,
- erweiterte Servicezeiten,
- 24×5,
- 24×7,
- Bereitschaft für kritische Services,
- oder unterschiedliche Zeiten nach Serviceklasse.

“ Wichtig

Eine längere Servicezeit benötigt nicht nur einen zusätzlichen Telefonanschluss.

Sie benötigt Personal, Wissen, Befugnisse, Werkzeuge, Eskalationswege und erreichbare Lieferanten.

Erreichbarkeit außerhalb der Servicezeit

Außerhalb der regulären Servicezeit sollte klar sein:

- Welche Anliegen werden bearbeitet?
- Welcher Kanal gilt?
- Wer reagiert?
- Welche Zielzeiten gelten?
- Welche Befugnisse besitzt die Bereitschaft?
- Welche Fachteams können erreicht werden?
- Welche Lieferanten stehen zur Verfügung?
- Wie erfolgt die Übergabe an den regulären Service Desk?

Mögliche Ansage:

“ Der reguläre Service Desk ist derzeit geschlossen. Kritische Ausfälle der Produktionsservices können über die Bereitschaftsnummer gemeldet werden. Alle anderen Anliegen können im Portal erfasst werden und werden ab 08:00 Uhr bearbeitet.

Bereitschaft und Rufbereitschaft

Eine Bereitschaftsregelung sollte mindestens klären:

- betroffene Services,
- Aktivierungsbedingungen,
- erreichbare Rollen,
- Reaktionspflichten,
- Entscheidungsbefugnisse,
- technische Zugänge,
- Dokumentation,
- Vertretung,
- und Übergabe.

Problematisch sind informelle Regelungen wie:

Rufen Sie einfach jemanden aus der IT an.

Dies führt zu:

- unklarer Verantwortung,
- persönlicher Überlastung,
- fehlender Vertretung,
- und nicht nachvollziehbaren Entscheidungen.

Follow-the-Sun

Bei internationalem Betrieb können Teams in verschiedenen Zeitzonen nacheinander übernehmen.

Voraussetzungen:

- einheitliche Dokumentation,
- gemeinsame Werkzeuge,
- klare Ownership-Regeln,
- definierte Übergaben,
- ausreichende Sprachkenntnisse,
- gleiche Zugriffsmöglichkeiten,
- und abgestimmte Prioritätskriterien.

Eine Übergabe sollte enthalten:

- aktueller Status,
- bisherige Maßnahmen,
- offene Hypothesen,
- nächste Schritte,
- Risiken,
- erwartete Entscheidungen,
- und geplante Kommunikation.

“ Typischer Fehler

Der Vorgang wird am Schichtende nur einer anderen Gruppe zugewiesen, ohne dass Kontext und Verantwortung geklärt sind.

Sprachliche Erreichbarkeit

Bei mehrsprachigen Benutzergruppen ist zu klären:

- Welche Sprachen werden direkt unterstützt?
- Welche Servicezeiten gelten je Sprache?
- Können Übersetzungswerkzeuge verwendet werden?
- Wie werden technische Begriffe einheitlich übersetzt?
- Wie werden Missverständnisse erkannt?
- Welche Sprache gilt für Dokumentation und Lieferanteneskalation?

Automatische Übersetzung kann unterstützen.

Kritische Informationen sollten jedoch überprüft werden, insbesondere bei:

- Sicherheitsvorfällen,
- rechtlichen Aussagen,
- technischen Anweisungen,
- und möglichen Datenverlusten.

Erreichbarkeit für externe Benutzer

Externe Kunden, Partner oder Lieferanten benötigen möglicherweise andere Kanäle als interne Mitarbeiter.

Zu berücksichtigen sind:

- Authentifizierung,
- Vertragsbezug,
- Mandantentrennung,
- Datenschutz,
- zulässige Informationen,
- Servicezeiten,
- Eskalation,
- und unterschiedliche Serviceziele.

Ein externer Benutzer sollte nicht auf interne Portale oder Kommunikationskanäle zugreifen müssen, für die er keine Berechtigung besitzt.

Identitätsprüfung je Kanal

Nicht jede Anfrage benötigt dieselbe Identitätsprüfung.

Der Umfang sollte sich nach Risiko und verlangter Handlung richten.

Beispiele:

Handlung	Mögliche Anforderung
allgemeine Serviceinformation	möglicherweise keine besondere Prüfung

Handlung	Mögliche Anforderung
Status eines eigenen Tickets	sichere Anmeldung oder Vorgangsprüfung
Kennwort zurücksetzen	festgelegtes starkes Identitätsverfahren
Berechtigung ändern	Identitäts- und Genehmigungsprüfung
vertrauliche Daten übermitteln	geschützter Kanal
administrativen Zugriff aktivieren	besonders starke Prüfung und Autorisierung

“ Sicherheitsrelevant

Telefonnummer, Absenderadresse oder angezeigter Name allein beweisen nicht zuverlässig die Identität einer Person.

Social Engineering berücksichtigen

Kontaktkanäle können durch Angreifer ausgenutzt werden.

Typische Warnzeichen:

- außergewöhnlicher Zeitdruck,
- Berufung auf hohe Hierarchie,
- Bitte um Umgehung des üblichen Verfahrens,
- Zurücksetzung eines fremden Kontos,
- Änderung von Kontaktdaten vor einer Sicherheitsaktion,
- Übermittlung unbekannter Links oder Dateien,
- oder Forderung nach vertraulichen Informationen.

Mitarbeiter benötigen:

- klare Verfahren,
- Schulung,
- Eskalationsmöglichkeiten,
- und Unterstützung durch Führungskräfte.

“ Grundsatz

Gute Erreichbarkeit darf nicht auf Kosten von Identitätsprüfung und Informationssicherheit entstehen.

Kapazitätsplanung für Kontaktkanäle

Ein Kanal ist nur dann zuverlässig, wenn ausreichende Kapazität vorhanden ist.

Zu berücksichtigen sind:

- Anzahl der Kontakte,
- zeitliche Verteilung,
- durchschnittliche Bearbeitungsdauer,
- saisonale Spitzen,
- Ausfälle größerer Services,
- Personalverfügbarkeit,
- Sprachen,
- und Komplexität der Anliegen.

Beispiele für Spitzen:

- Montagmorgen,
- Beginn einer Schicht,
- nach einem großen Release,
- nach Kennwortänderungen,
- bei neuen MitarbeiterEinstiegsterminen,
- oder während eines Major Incidents.

Mögliche Maßnahmen:

- Rückrufoption,
- zusätzliche Besetzung,
- sichtbare Statusmeldung,
- vorbereitete Störungsansage,
- Self-Service für geeignete Anliegen,
- und automatische Zusammenführung von Mehrfachmeldungen.

Warteschlangen steuern

Eine Warteschlange sollte nicht nur die Reihenfolge nach Eingangszeit berücksichtigen.

Abhängig vom Kanal können relevant sein:

- Priorität,
- Auswirkungen,
- Sicherheitsbezug,
- Serviceklasse,
- bereits verstrichene Zeit,
- Sprachbedarf,
- und benötigte Fähigkeiten.

Benutzer sollten möglichst erkennen können:

- dass ihre Meldung eingegangen ist,
 - ob weitere Informationen benötigt werden,
 - wie der nächste Schritt aussieht,
 - und wann ungefähr eine Reaktion erfolgt.
-

Überlauf und Ausweichregelungen

Bei ungewöhnlich hoher Nachfrage können Ausweichregeln notwendig sein.

Beispiele:

- zusätzliche interne Mitarbeiter unterstützen vorübergehend,
- nichtkritische Kontakte werden zurückgerufen,
- bekannte Störung wird zentral kommuniziert,
- Lieferanten übernehmen vereinbarte Teile,
- oder automatisierte Statusinformationen reduzieren Nachfragen.

Zu vermeiden ist:

- spontane Weitergabe ohne Zugriffsrechte,
 - Einsatz ungeschulter Personen bei sicherheitskritischen Anliegen,
 - und Verlust der Dokumentation.
-

Kontaktkanäle und Service Levels

Serviceziele können je Kanal und Anliegen unterschiedlich sein.

Beispiele:

- Telefon: kurze Annahmezeit für kritische Incidents
- Portal: Eingangsbestätigung unmittelbar
- E-Mail: qualifizierte Reaktion innerhalb der Servicezeit
- Chat: Reaktion nur während angezeigter Verfügbarkeit
- Bereitschaft: definierte Reaktion bei kritischen Services

Die Ziele sollten:

- verständlich,
- messbar,
- realistisch,
- und mit ausreichenden Ressourcen unterstützt

sein.

Eine sehr kurze Reaktionszeit besitzt wenig Wert, wenn die erste Antwort nur lautet:



Ihr Ticket wurde erhalten.

Zusätzlich sollte geprüft werden, wann:

- eine qualifizierte Bearbeitung,
- eine sinnvolle Statusinformation,
- oder eine Wiederherstellung

erfolgt.

Erreichbarkeit messen

Mögliche Kennzahlen:

Kennzahl	Mögliche Aussage
Erreichbarkeitsquote Telefon	Anteil angenommener Anrufe
durchschnittliche Wartezeit	Zeit bis zur Annahme
Abbruchquote	Anteil beendeter Kontakte vor Annahme
Rückrufzeit	Zeit bis zum zugesagten Rückruf
erste qualifizierte Reaktionszeit	Zeit bis zu einer verwertbaren Antwort
Portal-Abbruchquote	Anteil nicht abgeschlossener Formulare
Chat-Übertragungsquote	Anteil der Kontakte mit menschlicher Übergabe
Kanalwechselquote	Anteil der Fälle, die einen weiteren Kanal benötigen
Wiederholungskontakte	erneute Meldung zum selben Anliegen
Self-Service-Erfolgsquote	erfolgreich ohne Service-Desk-Kontakt erledigte geeignete Anliegen
Kontakte außerhalb Servicezeit	Hinweise auf unpassende Servicezeiten
falsch gewählter Kanal	Hinweise auf unklare Kommunikation
Benutzeraufwand	Anzahl notwendiger Kontakte oder Wiederholungen

Keine einzelne Kennzahl beschreibt die tatsächliche Erreichbarkeit vollständig.

Abbruchquote richtig einordnen

Eine hohe Abbruchquote kann entstehen durch:

- lange Wartezeit,
- technische Probleme,

- unverständliches Telefonmenü,
- Benutzer findet inzwischen eine Lösung,
- oder parallele Nutzung eines anderen Kanals.

Eine niedrige Abbruchquote beweist nicht automatisch gute Erreichbarkeit.

Möglicherweise:

- werden Anrufe schnell angenommen, aber schlecht bearbeitet,
- Benutzer verwenden den Kanal gar nicht mehr,
- oder kritische Gruppen können ihn nicht nutzen.

Kennzahlen müssen deshalb gemeinsam mit:

- Benutzerfeedback,
- Lösungsqualität,
- Kontaktvolumen,
- und tatsächlichen Outcomes

betrachtet werden.

First Contact Resolution nach Kanal

First Contact Resolution kann je Kanal unterschiedlich bewertet werden.

Beispiele:

- Chatbot beantwortet eine Statusfrage vollständig.
- Portal führt einen sicheren Kennwort-Reset aus.
- Telefonischer Mitarbeiter löst eine bekannte Störung.
- E-Mail liefert eine verständliche und erfolgreiche Anleitung.

Dabei muss geprüft werden:

- War das Anliegen tatsächlich gelöst?
- Wurde das Ergebnis bestätigt?
- Musste der Benutzer einen weiteren Kanal verwenden?
- Wurden Sicherheitsregeln eingehalten?
- Wurde nur das Ticket geschlossen oder das Outcome erreicht?

Self-Service-Erfolg richtig messen

Unzureichende Kennzahl:



Hilfreichere Fragen:

- Finden Benutzer das passende Angebot?
- Werden Formulare vollständig abgeschlossen?
- Wird das Anliegen ohne weiteren Kontakt erledigt?
- Sind die Ergebnisse korrekt?
- Wie häufig wechseln Benutzer zum Telefon?
- Welche Suchbegriffe liefern keine Ergebnisse?
- Wo brechen Benutzer ab?
- Welche Fehler verursachen neue Tickets?

“ Merke

Ein Benutzer, der nach mehreren erfolglosen Self-Service-Versuchen anruft, hat mehr und nicht weniger Aufwand erlebt.

Kanalqualität regelmäßig überprüfen

Kontaktkanäle verändern sich durch:

- neue Benutzergruppen,
- neue Technologien,
- veränderte Arbeitszeiten,
- steigende Kontaktmengen,
- neue Sicherheitsrisiken,
- und Feedback.

Regelmäßig zu prüfen sind:

- Werden alle Kanäle noch benötigt?
 - Sind Servicezeiten passend?
 - Sind Inhalte und Ansagen aktuell?
 - Werden Kontakte zuverlässig zusammengeführt?
 - Funktionieren Übergaben?
 - Gibt es ungenutzte oder überlastete Kanäle?
 - Bestehen unnötige parallele Wege?
 - Sind alternative Kanäle vorbereitet?
 - Ist die Benutzererfahrung verständlich?
 - Sind Sicherheitsmaßnahmen ausreichend?
-

Kanäle nicht nur hinzufügen, sondern auch entfernen

Neue Kanäle werden häufig schnell ergänzt.

Alte Kanäle bleiben jedoch bestehen.

Dadurch können entstehen:

- unklare Auswahl,
- veraltete Adressen,
- schlecht überwachte Postfächer,
- widersprüchliche Informationen,
- und zusätzlicher Betriebsaufwand.

Vor der Abschaltung eines Kanals sollte geprüft werden:

- Wer verwendet ihn?
- Welche Benutzergruppe wäre betroffen?
- Welche Alternative besteht?
- Wie wird die Änderung kommuniziert?
- Müssen Weiterleitungen eingerichtet werden?
- Gibt es vertragliche oder betriebliche Anforderungen?
- Wie lange bleibt ein Übergangszeitraum bestehen?

Einführung eines neuen Kanals

Eine mögliche Vorgehensweise:

1. Benutzerbedarf und Problem beschreiben
2. geeignete Anwendungsfälle festlegen
3. Sicherheits- und Datenschutzanforderungen prüfen
4. Verantwortlichkeit bestimmen
5. technische Integration planen
6. Servicezeiten und Kapazität festlegen
7. Pilotgruppe auswählen
8. Erfolgskriterien definieren
9. Mitarbeiter und Benutzer informieren
10. Ergebnisse messen
11. Kanal anpassen oder ausweiten
12. bestehende Kanäle erneut bewerten

Beispiel:

Ein Chatkanal sollte nicht nur deshalb eingeführt werden, weil die verwendete Plattform diese Funktion anbietet.

Zu prüfen ist:

- Welche Anliegen sollen über Chat laufen?
 - Wer besetzt ihn?
 - Wird der Verlauf dokumentiert?
 - Wie erfolgt die Identitätsprüfung?
 - Wie wird an Fachteams übergeben?
 - Wann wird der Chat geschlossen?
 - Wie wird eine hohe gleichzeitige Nachfrage behandelt?
-

Kontaktkanäle bei einem Major Incident

Während eines Major Incidents kann das Kontaktvolumen stark steigen.

Geeignete Maßnahmen:

- bekannte Störung sichtbar veröffentlichen,
- automatische Ansage aktualisieren,
- identische Meldungen verknüpfen,
- Service-Desk-Mitarbeitern freigegebene Statusinformationen bereitstellen,
- klaren Aktualisierungsrhythmus festlegen,
- und einen separaten technischen Koordinationskanal verwenden.

Benutzerkanal und technischer Koordinationskanal sollten unterschieden werden.

Benutzerkanal

- verständliche Statusinformation
- Auswirkungen
- Zwischenlösung
- nächste Aktualisierung

Technischer Koordinationskanal

- Diagnose,
- Hypothesen,
- technische Maßnahmen,
- Entscheidungen,
- Risiken,
- und Verantwortlichkeiten

Technische interne Diskussionen sollten nicht ungefiltert in öffentliche Statusmeldungen übernommen werden.

Kontaktkanäle bei Sicherheitsvorfällen

Bei einem möglichen Sicherheitsvorfall können zusätzliche Anforderungen gelten.

Beispiele:

- vertrauliche Behandlung,
- begrenzter Zugriff,
- Beweissicherung,
- keine öffentliche Statusmeldung,
- definierte Meldepflichten,
- und besonders kontrollierte Kommunikation.

Der normale Service Desk kann den ersten Kontakt aufnehmen.

Er muss jedoch wissen:

- wann das Sicherheitsteam einzubinden ist,
- welche Informationen nicht verändert werden dürfen,
- welche Kanäle zulässig sind,
- und welche Aussagen vermieden werden müssen.

Kontaktkanäle bei Service Requests

Standardisierte Service Requests eignen sich häufig gut für Portale und Automatisierung.

Beispiele:

- Standardsoftware anfordern,
- Gruppenmitgliedschaft beantragen,
- neues Zubehör bestellen,
- Verteilerliste ändern,
- oder Arbeitsplatzwechsel melden.

Ein gutes Request-Formular kann:

- benötigte Informationen erfassen,
- Genehmigung automatisch anstoßen,
- den Status sichtbar machen,
- und standardisierte Erfüllung auslösen.

Der Benutzer sollte erkennen können:

- welche Voraussetzungen gelten,
 - welche Kosten entstehen können,
 - welche Genehmigung benötigt wird,
 - und welche Bereitstellungszeit zu erwarten ist.
-

Kontaktkanäle beim Onboarding

Beim Onboarding entstehen häufig mehrere Kontakte:

- Personalabteilung meldet den Eintritt.
- Führungskraft nennt Rolle und Zugriffe.
- Einkauf oder Asset Management stellt Geräte bereit.
- neuer Mitarbeiter erhält Informationen.
- Service Desk unterstützt bei der ersten Nutzung.

Ein zentraler digitaler Einstieg kann helfen, Informationen einmalig und strukturiert zu erfassen.

Dabei muss geklärt sein:

- Wer darf den Eintritt melden?
- Welche Daten werden benötigt?
- Welche Freigaben gelten?
- Wie wird der Status sichtbar?
- Wie erhält der neue Mitarbeiter Unterstützung, wenn das Konto noch nicht funktioniert?

Der letzte Punkt ist besonders wichtig.

Ein ausschließlich internes Portal ist möglicherweise nicht nutzbar, wenn der Benutzer noch keinen funktionierenden Zugang besitzt.

Praxisbeispiel: Portal wird kaum verwendet

Beobachtung

- Benutzer rufen fast immer an.
- Das Portal besitzt viele Formulare.
- Suchbegriffe führen zu unpassenden Ergebnissen.
- Benutzer kennen die Bearbeitungszeiten nicht.

Ungeeignete Reaktion

“ Ab nächster Woche werden telefonische Anfragen nicht mehr angenommen.

Bessere Untersuchung

- Welche Anliegen werden telefonisch gemeldet?
- Können Benutzer die passenden Portalangebote finden?
- Welche Formulare werden abgebrochen?
- Sind technische Begriffe verständlich?

- Funktioniert die Anmeldung zuverlässig?
- Ist das Portal mobil verwendbar?
- Gibt es einen menschlichen Ausweichweg?
- Welchen Nutzen besitzt das Portal für den Benutzer?

Mögliche Verbesserungen

- häufige Angebote hervorheben,
 - Begriffe vereinfachen,
 - Formulare kürzen,
 - Suche verbessern,
 - Statusinformationen ergänzen,
 - Anmeldung vereinfachen,
 - und Portal gemeinsam mit Benutzern testen.
-

Praxisbeispiel: Zu viele E-Mail-Tickets

Beobachtung

- Viele E-Mails besitzen keinen eindeutigen Betreff.
- notwendige Informationen fehlen.
- mehrere Personen antworten parallel.
- Anhänge enthalten sensible Daten.

Mögliche Verbesserungen

- automatische Eingangsbestätigung,
- kurze Hinweise zu benötigten Angaben,
- sichere Uploadmöglichkeit,
- automatische Verknüpfung mit bestehenden Vorgängen,
- verständliches Portal als Alternative,
- und Schulung des Service Desk zur Nachqualifizierung.

E-Mail muss nicht zwingend abgeschafft werden.

Sie kann für bestimmte Benutzergruppen weiterhin ein sinnvoller Kanal sein.

Praxisbeispiel: Support außerhalb der Geschäftszeit

Ausgangslage

- Produktionsservice läuft rund um die Uhr.
- Service Desk arbeitet von 08:00 bis 18:00 Uhr.
- Nachts rufen Benutzer private Telefonnummern von Administratoren an.

Möglicher Zielzustand

- definierte Bereitschaftsnummer,
- klare Kriterien für kritische Meldungen,
- erreichbarer Incident-Koordinator,
- aktueller Dienstplan,
- dokumentierte Übergabe,
- und Portal für nichtkritische Anliegen.

Zusätzlich zu klären

- Welche technischen Teams müssen erreichbar sein?
 - Welche Lieferanten bieten Nachtsupport?
 - Welche Maßnahmen darf die Bereitschaft durchführen?
 - Wer darf risikobehaftete Entscheidungen treffen?
 - Wie erfolgt die Information der regulären Teams?
-

Praxisbeispiel: Virtueller Agent blockiert Benutzer

Ausgangslage

- Chatbot beantwortet Standardfragen.
- Benutzer kann keinen Mitarbeiter auswählen.
- Nach drei nicht passenden Antworten beginnt der Dialog erneut.
- Benutzer ruft anschließend verärgert an.

Mögliche Verbesserungen

- menschliche Übergabe sichtbar anbieten,
- bisherigen Verlauf übertragen,
- Abbruchgründe analysieren,
- Wissensquellen verbessern,
- ungeeignete Anwendungsfälle entfernen,
- und kritische Begriffe sofort eskalieren.

“ Merke

Automatisierung soll einen Kontakt vereinfachen und nicht als Barriere vor menschlicher Unterstützung dienen.

Praxisbeispiel: Ticketsystem fällt aus

Situation

- Service-Desk-Portal und Ticketsystem sind nicht erreichbar.
- E-Mail-Tickets können ebenfalls nicht verarbeitet werden.
- Benutzer benötigen weiterhin einen Meldeweg.

Vorbereitete Lösung

- unabhängige Notfallnummer,
- vorübergehende gesicherte Erfassung,
- externe Statusseite,
- definierte Priorisierung,
- und spätere Übernahme der Notfallvorgänge in das Ticketsystem.

Zu vermeiden:

- private Notizzettel ohne spätere Übernahme,
- unkontrollierte Chatgruppen,
- und Veröffentlichung interner technischer Details.

Typische Fehler bei Kontaktkanälen

Fehler 1: Möglichst viele Kanäle anbieten

Die Organisation kann sie nicht zuverlässig überwachen und zusammenführen.

Fehler 2: Portalzwang ohne geeignete Alternative

Komplexe, dringende oder barrierebedingte Situationen werden nicht berücksichtigt.

Fehler 3: Technische Verfügbarkeit mit Supportzeit verwechseln

Benutzer erwarten sofortige Bearbeitung, obwohl nur eine automatische Erfassung erfolgt.

Fehler 4: Private Supportkanäle dulden

Meldungen verschwinden in persönlichen Chats, Postfächern oder Telefonlisten.

Fehler 5: Benutzer müssen das technische Team auswählen

Falsche Zuordnungen und unnötige Weiterleitungen entstehen.

Fehler 6: Kritische und normale Anliegen verwenden denselben unpriorisierten Kanal

Dringende Meldungen werden möglicherweise zu spät erkannt.

Fehler 7: Kein alternativer Kanal

Beim Ausfall von Portal, E-Mail oder Identitätsdienst ist der Service Desk nicht erreichbar.

Fehler 8: Virtueller Agent ohne menschlichen Ausweg

Benutzer bleiben in automatisierten Antwortschleifen.

Fehler 9: Kanäle werden nicht sicher gestaltet

Identitätsprüfung, Datenschutz und vertrauliche Kommunikation fehlen.

Fehler 10: Servicezeiten sind nicht sichtbar

Benutzer wissen nicht, wann mit einer Reaktion zu rechnen ist.

Fehler 11: Kanalwechsel verliert den Kontext

Benutzer müssen ihre Situation mehrfach erklären.

Fehler 12: Self-Service nur zur Kostensenkung

Benutzeraufwand und Abbruchquote steigen.

Fehler 13: Statusseite wird nicht aktualisiert

Veraltete Informationen beschädigen das Vertrauen.

Fehler 14: Bereitschaft ist nur informell geregelt

Einzelne Mitarbeiter werden unkoordiniert und ohne Vertretung kontaktiert.

Fehler 15: Kennzahlen werden isoliert optimiert

Kurze Wartezeiten werden erreicht, während Lösungsqualität und Benutzererfahrung sinken.

Bedeutung für Fachinformatiker für Systemintegration

Fachinformatiker arbeiten häufig in Service Desk, Betrieb oder nachgelagerten Supportgruppen.

Sie sollten die vorgesehenen Kontaktwege kennen und unterstützen.

Wichtige Verhaltensweisen:

- private Meldungen in den offiziellen Wertstrom überführen,
- kritische Anliegen nicht wegen eines falschen Kanals ignorieren,
- technische Rückmeldungen im zentralen Vorgang dokumentieren,
- Benutzer nicht unnötig an einen weiteren Kanal verweisen,
- alternative Meldewege bei Ausfällen kennen,
- Sicherheitsverfahren einhalten,
- und Statusinformationen an den Service Desk zurückgeben.

Beispiel:

Ein Benutzer schreibt einem Administrator direkt:

“ Der Fileserver geht nicht.

Ungeeignet:

“ Dafür bin ich nicht zuständig. Eröffnen Sie ein Ticket.

Besser:

“ Ich erfasse die Meldung im Service Desk, damit sie nachvollziehbar bearbeitet wird. Können Sie mir kurz sagen, ob nur Sie oder weitere Benutzer betroffen sind?

Anschließend:

- Vorgang erstellen,
- Auswirkung prüfen,
- zuständige Bearbeitung einbinden,
- und Benutzer über den nächsten Schritt informieren.

30-Sekunden-Prüfung eines Kontaktkanals

1. **Zielgruppe:** Wer soll den Kanal verwenden?
2. **Anliegen:** Für welche Kontakte ist er geeignet?
3. **Servicezeit:** Wann wird er tatsächlich bearbeitet?

4. **Verantwortung:** Wer überwacht den Kanal?
 5. **Integration:** Werden Kontakte zentral dokumentiert?
 6. **Sicherheit:** Wie werden Identität und Informationen geschützt?
 7. **Barrierefreiheit:** Können die vorgesehenen Benutzer den Kanal verwenden?
 8. **Eskalation:** Wie gelangen kritische Anliegen schnell zur richtigen Stelle?
 9. **Alternative:** Was geschieht bei Ausfall des Kanals?
 10. **Übergabe:** Bleiben Informationen bei einem Kanalwechsel erhalten?
 11. **Messung:** Wie wird die Wirksamkeit überprüft?
 12. **Verbesserung:** Wie wird Benutzerfeedback verwendet?
-

Checkliste für ein Self-Service-Portal

- ☐ Sind häufige Anliegen leicht auffindbar?
 - ☐ Werden verständliche Begriffe verwendet?
 - ☐ Müssen Benutzer keine internen Teams oder Practices kennen?
 - ☐ Sind Formulare so kurz wie möglich?
 - ☐ Werden nur notwendige Informationen verlangt?
 - ☐ Sind Servicezeiten und erwartete Bearbeitungszeiten sichtbar?
 - ☐ Ist der Status eines Vorgangs nachvollziehbar?
 - ☐ Funktioniert das Portal auf benötigten Geräten?
 - ☐ Sind barrierearme Nutzung und Alternativen berücksichtigt?
 - ☐ Ist ein menschlicher Kontaktweg sichtbar?
 - ☐ Werden Sicherheits- und Datenschutzerfordernungen eingehalten?
 - ☐ Werden Suchbegriffe, Abbrüche und Feedback ausgewertet?
-

Checkliste für telefonischen Support

- ☐ Ist die Nummer leicht auffindbar?
 - ☐ Sind Servicezeiten veröffentlicht?
 - ☐ Ist die Ansage verständlich und aktuell?
 - ☐ Ist das Telefonmenü möglichst kurz?
 - ☐ Besteht eine Regel für kritische Incidents?
 - ☐ Werden Kontakte zentral dokumentiert?
 - ☐ Ist die Identitätsprüfung risikogerecht?
 - ☐ Bestehen Rückruf- oder Überlaufmöglichkeiten?
 - ☐ Sind Wartezeiten und Abbruchquoten bekannt?
 - ☐ Ist eine Vertretung bei Ausfall der Telefonanlage vorbereitet?
-

Checkliste für E-Mail-Support

- ☐ Wird ein gemeinsames statt eines privaten Postfachs verwendet?
 - ☐ Erfolgt eine automatische Eingangsbestätigung?
 - ☐ Wird eine Vorgangsnummer erzeugt?
 - ☐ Sind Servicezeiten und dringende Alternativen angegeben?
 - ☐ Werden Anhänge sicher verarbeitet?
 - ☐ Sind Regeln für vertrauliche Informationen vorhanden?
 - ☐ Werden E-Mail-Verläufe dem richtigen Vorgang zugeordnet?
 - ☐ Werden Duplikate erkannt?
 - ☐ Ist der Kanal regelmäßig überwacht?
 - ☐ Werden unvollständige Meldungen strukturiert nachqualifiziert?
-

Checkliste für Chat und virtuelle Agenten

- ☐ Ist erkennbar, ob ein Mensch oder ein automatisiertes System antwortet?
 - ☐ Sind die Servicezeiten sichtbar?
 - ☐ Wird der Verlauf dokumentiert?
 - ☐ Können Vorgänge automatisch erzeugt werden?
 - ☐ Besteht ein klarer Übergang zu einem Menschen?
 - ☐ Bleiben Informationen bei der Übergabe erhalten?
 - ☐ Werden kritische und sicherheitsbezogene Begriffe erkannt?
 - ☐ Ist die Identitätsprüfung für sensible Aktionen ausreichend?
 - ☐ Werden Fehlantworten und Abbrüche ausgewertet?
 - ☐ Werden Benutzer nicht in Antwortschleifen festgehalten?
-

Checkliste für Erreichbarkeit außerhalb der Servicezeit

- ☐ Ist bekannt, welche Services kritisch sind?
- ☐ Sind Aktivierungskriterien für die Bereitschaft definiert?
- ☐ Ist der Meldeweg veröffentlicht?
- ☐ Ist ein aktueller Dienstplan vorhanden?
- ☐ Besitzen Bereitschaftskräfte notwendige Zugänge und Befugnisse?
- ☐ Sind technische Eskalationswege bekannt?
- ☐ Sind Lieferanten außerhalb der Geschäftszeit erreichbar?
- ☐ Besteht ein alternativer Kanal bei Systemausfall?

- ☐ Werden alle Maßnahmen dokumentiert?
- ☐ Ist die Übergabe an den regulären Service Desk geregelt?

Checkliste für die gesamte Kanalstrategie

- ☐ Sind Benutzergruppen und ihre Arbeitsbedingungen bekannt?
- ☐ Sind geeignete Kanäle für unterschiedliche Anliegen definiert?
- ☐ Werden alle Kanäle zuverlässig überwacht?
- ☐ Werden Kontakte in einer gemeinsamen Sicht zusammengeführt?
- ☐ Sind Servicezeiten eindeutig veröffentlicht?
- ☐ Sind kritische und normale Anliegen unterscheidbar?
- ☐ Sind Sicherheits- und Datenschutzerfordernungen berücksichtigt?
- ☐ Bestehen barrierearme und alternative Kontaktmöglichkeiten?
- ☐ Bleibt der Kontext bei Kanalwechseln erhalten?
- ☐ Ist der Service Desk auch bei Ausfall zentraler Systeme erreichbar?
- ☐ Sind Kapazität und Bereitschaft ausreichend?
- ☐ Sind Statusinformationen konsistent?
- ☐ Werden Kennzahlen und Benutzerfeedback gemeinsam ausgewertet?
- ☐ Werden ungenutzte oder ungeeignete Kanäle entfernt?
- ☐ Fließen Erkenntnisse in Continual Improvement ein?

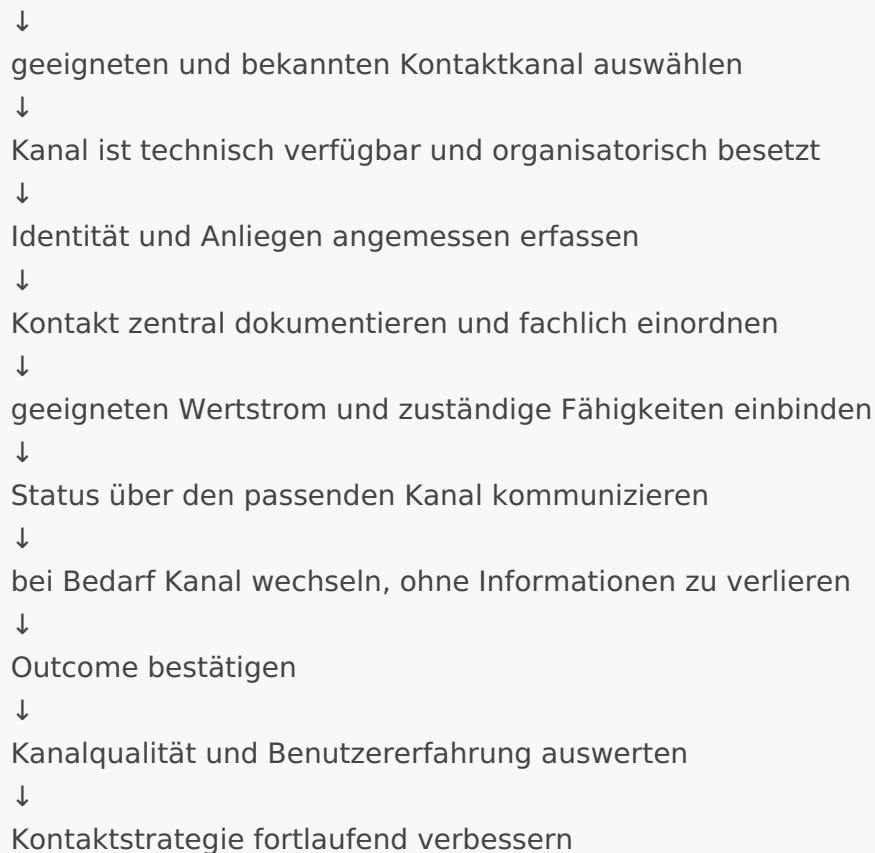
Schnellreferenz

Kanal	Besonders geeignet für	Besonders zu beachten
Portal	strukturierte Incidents und Requests	Verständlichkeit, Suche und Alternativkanal
Telefon	dringende und komplexe Situationen	Wartezeit, Dokumentation und Identitätsprüfung
E-Mail	schriftliche, weniger dringende Anliegen	Vollständigkeit, Anhänge und Sicherheit
Chat	schnelle Rückfragen und begleitete Diagnose	Dokumentation und Übergabe
virtueller Agent	häufige standardisierte Anliegen	Transparenz, Qualität und menschlicher Ausweg
mobile App	mobile Benutzer und Statusinformationen	Gerätesicherheit und Datenschutz

Kanal	Besonders geeignet für	Besonders zu beachten
Vor-Ort-Kontakt	Geräteprobleme und komplexe Unterstützung	Dokumentation und Priorisierung
Notfallkanal	klar definierte kritische Situationen	Missbrauchsschutz und schnelle Eskalation
Statusseite	bekannte Störungen und Wartungen	Aktualität und Schutz vertraulicher Informationen

Zusammenfassende Darstellung

“ Benutzer benötigt Unterstützung



Verwandte Seiten

- 3.1 Der Service Desk als zentraler Kontaktpunkt
- 3.3 Benutzerkommunikation und professioneller Umgang
- 3.4 Tickets vollständig erfassen und kategorisieren
- 3.5 Auswirkungen, Dringlichkeit und Priorität
- 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
 - Knowledge Management
 - Service Level Management
 - Service Continuity Management
-

Quellen und Versionsstand

Offizielle Grundlagen

- [PeopleCert: ITIL 4 Practitioner – Service Desk](#)
- [PeopleCert: ITIL 4 Practitioner – Service Desk Mock Exam](#)
- [ITIL: The ongoing relevance of the service desk in an AI world](#)
- [PeopleCert: Build an AI-Powered Service Desk That Runs Itself](#)
- [ITIL: ITIL Service – Version 5](#)
- [PeopleCert: ITIL Foundation – Version 5](#)

Offiziell bestätigter Stand

Die offiziellen ITIL- und PeopleCert-Quellen bestätigen:

- Der Service Desk dient als zentraler Kontaktpunkt zwischen Service Provider und Benutzern.
- Eine wirksame Service-Desk-Practice beeinflusst Benutzererfahrung, Kundenerfahrung und Servicebeziehungen.
- Informationen und Technologien sollen die Service-Desk-Practice unterstützen, Arbeitsweisen vereinfachen und Benutzererfahrung verbessern.
- Virtuelle Service Desks, KI-gestützte Unterstützung, Chatbots und automatisierte Standardaufgaben sind heute verbreitete Bestandteile moderner Serviceumgebungen.
- Menschliche Kommunikation, Empathie, Kontextverständnis und kreative Zusammenarbeit bleiben insbesondere bei komplexen Situationen wichtig.
- Self-Service sollte durch verständliche Portale, hochwertige Wissensinhalte, Vertrauen und benutzerorientierte Gestaltung unterstützt werden.
- ITIL Version 5 richtet Serviceaktivitäten stärker auf Endbenutzererfahrung, Wertfluss und Zusammenarbeit über organisatorische Grenzen hinweg aus.

Einordnung

Die auf dieser Seite beschriebenen:

- Kanalmodelle,
- Servicezeiten,

- Bereitschaftsregelungen,
- Telefon- und Portalgestaltungen,
- Checklisten,
- Sicherheitsmaßnahmen,
- Kennzahlen,
- und Praxisbeispiele

sind herstellerneutrale redaktionelle Empfehlungen dieses unabhängigen Nachschlagewerks.

ITIL schreibt keine universelle:

- Anzahl von Kontaktkanälen,
- rund um die Uhr bestehende Servicezeit,
- Telefonmenüstruktur,
- Antwortzeit,
- Support-Level-Struktur,
- oder bestimmte technische Plattform

vor.

Die konkrete Kanalstrategie muss an:

- Benutzergruppen,
- Servicekritikalität,
- Arbeitszeiten,
- Risiken,
- Sicherheitsanforderungen,
- vertragliche Verpflichtungen,
- verfügbare Fähigkeiten,
- und organisatorische Ressourcen

angepasst werden.

Behandelter Framework-Stand: ITIL Version 5

Zusätzlich berücksichtigt: aktuelle öffentlich zugängliche ITIL-4-Service-Desk-Guidance

Fachlicher Stand: August 2026
