

Ausarbeitung zum Thema:

Incident Management

Fachhochschule Furtwangen
Fachbereich Informatik
Studiengang Allgemeine Informatik
Anatolij Ristok, AI 7

Incident Management

Einführung

Übersetzt aus dem Englischen bedeutet incident eine Störung bzw. ein Vorfall.

Ein Vorfall ist in erster Linie ein Ereignis. Diese Ereignisse ergeben sich meistens durch aufgetretene Fehler, Ausfälle oder auch einfache Anfragen. So ein Ereignis ist in der Regel die Ursache für die Minderung des standardmäßigen Betriebs eines Services. Zusätzlich können diese Ereignisse sogar zu einer Unterbrechung des standardmäßigen Betriebs eines Services führen.

Aufgrund ihrer Entstehungsursache kann z.B. ein IT-Unternehmen folgende Kategorien von Vorfällen unterscheiden:

- Applikation
- Hardware
- Service Requests (Spezielle Störungen/Vorfälle: Informationen und Anfragen zur Verbesserung oder Ausweitung von Serviceleistungen, haben keinen Einfluss auf die Verfügbarkeit des Service)

Einige Beispiele von Vorfällen:

- Applikation
 - Funktion nicht vorhanden
 - Fehler in Applikation
 - Ressourcenknappheit festgestellt
- Hardware
 - Systemabsturz
 - Automatischer Warntonsignal
 - Drucker funktioniert nicht
 - Kein Zugriff auf Konfiguration
- Service Requests
 - Information-, Dokumentation-, Mitteilungsanfragen
 - Passwort vergessen

Service Requests sind Anfragen, die keine Beeinträchtigung oder Unterbrechung des Servicebetriebs verursachen (z. B. Anforderungen allgemeiner Informationen).

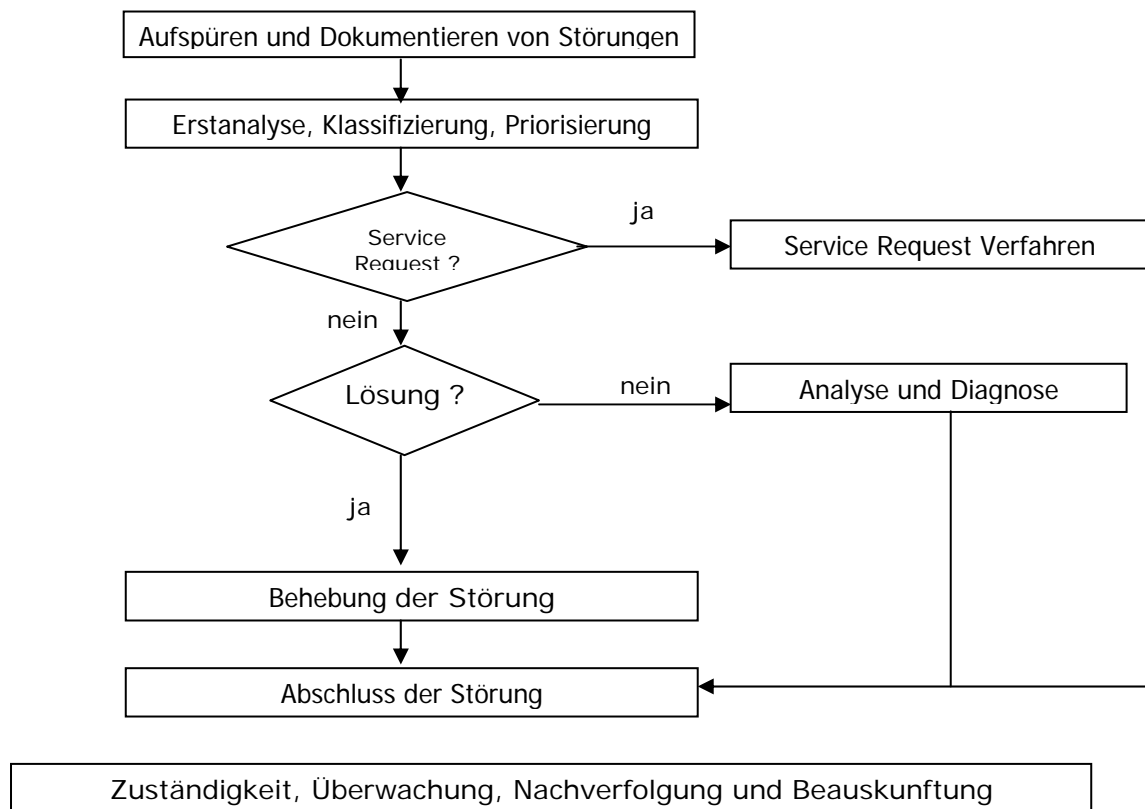
Zu den allgemeinen Aufgaben des Incident Managements gehören:

- Bestmögliche Verfügbarkeit des Services soll gewährleistet werden
- Dabei soll im Störfall schnellstmögliche Wiederherstellung des normalen Servicebetriebs durch Einleitung entsprechender Maßnahmen erreicht werden
- Beeinträchtigungen des Geschäftsbetriebs möglichst gering halten
- Service Desk ist Funktion innerhalb des Incident Managements
 - Operative Steuerung von Aktivitäten
 - Dokumentation von Aktivitäten (Incident Records)

Incident Management Process, Incident Lifecycle

Incident Management Process und Incident Lifecycle geben gemeinsam einen genaueren Überblick über Prozesse innerhalb sowie die Aufgaben des Incident Managements und durchzuführende Aktivitäten im Falle einer Störung.

Schaubild: Incident Management Process, Incident Lifecycle



Der Incident Management Prozess beginnt mit der Erfassung von Störungsinformationen durch den Service Desk.

Einige Unternehmen benutzen zur Sortierung von Anfragen ein vorgeschaltetes Dispatching-System (z.B. telefonische Eingabe von Ziffern trifft grundlegende Vorauswahl und später ggf. sogar automatische Standardansage). Dies entlastet die Mitarbeiter des Service-Desk, ergibt aber manchmal Kritik, wenn Benutzerführung nicht logisch ist oder den Kunden missfällt.

Im nächsten Schritt werden alle notwendigen Informationen über eine Störung gesammelt, die für weitere Prozesse zur Behandlung und Behebung der Störung wichtig sind. Dazu gehören z.B. das Datum und Symptome der Störung, Kontaktinformationen des Kunden, der die Störung „ausgelöst“ hat und weitere Details. Die Störungsinformationen werden in Form von Incident Records in das System aufgenommen und bleiben für ganze Dauer des Incident Lifecycle erhalten. Ursprüngliche Beschreibung von Symptomen einer Störung werden ebenfalls behalten.

Falls es sich bei der dokumentierten Störung um ein Service Request handelt, dann wird das Service Request – Verfahren, welches vom IT-Unternehmen selbst definiert werden kann, angestoßen.

Durch Priorisierung von Störungen ist es für weitere Stufe des Supports möglich, festzustellen, welche Störungen in welcher Reihenfolge zu bearbeiten sind, aber auch die erforderlichen Ressourcen. Incident Number wird vergeben und ebenfalls dokumentiert.

Abgleich der Störung mit Daten aus Known Error Database, Problem Database, Incident Database bezüglich Lösungen, Work-arounds oder ähnlichen Störungssymptomen soll weitere Aktionen einleiten. Falls Lösung oder Work-around existiert wird die Störung abgeschlossen, sonst aber auch an das nächste Support Level weitergeleitet/delegiert. Können die Spezialisten keine Lösung finden sollte ebenfalls auch nach einem Work-around gesucht werden, um die Arbeit der Kunden möglichst minimal zu unterbrechen. Nach der Lösung/Beseitigung der Störung muss diese abgeschlossen werden.

Von den Mitarbeitern des Service Desk werden sowohl fachliche Kenntnisse als auch kommunikative Fähigkeiten gefordert. Diese Punkte sind für die Beurteilung der Servicequalität durch den Kunden entscheidend. Erfahrungen zeigen, dass Mehrheit aller in Service Desk registrierter Störungen auch dort gelöst bzw. behoben werden (ca. 85%).

Die Gestaltung und Anpassung des Incident Management Prozesse wird durch die Person „Incident-Manager“ festgelegt. Er ist für den gesamten Incident Prozess sowie dessen Ergebnisse verantwortlich.

Kontinuierlicher Informationstausch mit dem Kunden wird während des gesamten Incident Lifecycle praktiziert. Alle geöffneten Störungen werden durch Incident Management überwacht.

Hauptaufgaben des Incident Managements (Zusammenfassung):

- Zuständigkeit für gesamten Lifecycle übernehmen
- Störungen/Vorfälle aufspüren, dokumentieren
- Störungen/Vorfälle klassifizieren, priorisieren
- Erstanalyse und First Level Support
- (bei schwierigen Störungen oder Überschreitung von Leistungsvereinbarungen (z.B. Zeit, Geld) wird Eskalation durchgeführt)
- Behebung der Störung, Servicewiederherstellung
- Überwachung, Nachverfolgung, akt. Beauskunftung zur Störungssachlage
- Abschluss von Störungsvorgängen, Reports und Auswertungen, um Service-Qualität zu verbessern

n-Level Support

Der Support wird personell von einem virtuellen Team durchgeführt. Bei dem Begriff „Virtuelles Team“ handelt es sich dabei nicht zwingend um eine permanente Einrichtung im Sinne einer eigenen Abteilung voller Spezialisten, sondern dass das Team durchaus flexibel und temporär, so zu sagen „On Demand“, beliebig aus internen und externen Fachkräften gebildet werden kann. Entscheidend ist dabei letztlich nur, dass der jeweils aktuell für die Lösung eines Problems benötigte Support Level verfügbar ist.

Das Spezialistenteam bildet eine dreistufige, im Spezialisierungsgrad gestaffelte Support Struktur:

- First Level Support
- Second Level Support
- Third Level Support

Alle erforderlichen Themenschwerpunkte werden damit parallel in unterschiedlichen fachlichen Tiefen abgebildet. Dies gewährleistet eine äußerst effiziente Störungsbearbeitung.

Der First Level Support dient als „erste Hilfe“-Maßnahme zur sofortigen Behebung einfacher Störungen und wird im Allgemeinen bereits im Rahmen des Service Desk erbracht. Kann die Störung an dieser Stelle nicht mit vertretbarem Aufwand behoben werden, wird sie zur weiteren Bearbeitung an den Second Level Support weitergeleitet.

Im Second Level Support wird dann mit tiefergehendem Fachwissen und entsprechender technischer Ausstattung, intensiv nach den Störungsursachen gesucht und Lösungsmöglichkeiten erarbeitet.

Sollte auch der Second Level Support nicht in der Lage sein, ein Problem im Rahmen seiner Möglichkeiten in den Griff zu bekommen, wird der Third Level Support hinzugezogen. Meistens handelt es sich dabei um so schwer wiegende Fehler, die nur noch vom Produkthersteller beseitigt werden können. In der Regel sind daher die Produkthersteller wichtiger Komponenten durch so genannte Underpinning Contracts (UC) direkt in den Third Level Support eingebunden.

Eine Weiterleitung einer Störung von einem Support Level zum nächsten wird als fachliche Eskalation bezeichnet. Bei fachlicher (=funktionale, =horizontale) Eskalation werden dem Incident Management zugeordnete Spezialisten (Team) zur Behebung der Störung hinzugezogen. Mögliche Gründe für fachliche Eskalationen: Mangel an Fachwissen, Überschreitung von Zeitvorgaben u.a. Dies geschieht meist automatisch.

Bei hierarchischer Eskalation werden zur Behebung der Störung die Mitarbeiter und Manager anderer Hierarchieebenen hinzugezogen. Im Gegensatz zur fachlichen Eskalation kann hierarchische jederzeit erfolgen und wird meist manuell ausgelöst. Gründe: Aufwandsüberlegungen und mögliche Gefahren für den Servicebetrieb.

Dokumentation von Störungen

Alle im Service Desk registrierten Störungen werden in Form so genannter Incident Records in einer Datenbank (Incident Database) gespeichert. Detaillierte Informationen über Störungen können auch von ereignisgesteuerten Management-Systemen stammen. Informationen werden meist effizient von Systemüberwachungswerkzeugen erledigt.

Es ist wichtig, dass alle Informationen einer Störung während des gesamten Incident Lifecycle erhalten bleiben. Dies ist von Vorteil, da das Support Team dadurch den Kunden über den aktuellen Stand der Störungsbehandlung informieren kann.

Folgende Daten sollten in/zum Incident Records aufgenommen werden:

- Einheitliche Referenznummer
- Klasse
- Eingangsdatum und Zeit
- Person (ID), die Störung aufgenommen hat
- Kontaktinformationen des Kunden
- Beschreibung der Störungssymptome des Kunden
- Priorität
- Status
- Zugehöriger CI
- Support Team/Person
- Zugehörige Probleme oder Bekannte Fehler
- Lösungsdatum und Zeit
- Anschlussdatum und Zeit

Störungen können in Abhängigkeit ihrer Behandlung verschiedene Statusinformationen zugewiesen werden:

- Neu
- Akzeptiert
- In Arbeit
- Angehalten
- Gelöst
- Abgeschlossen
- u.a.

Folgende Informationen einer Störung können sich im Verlaufe des Incident Lifecycle ändern:

- Historie
- Status
- Priorität
- Zeitaufwand und Kosten
- Informationen über Eskalation/Delegierung
- Name der Person, die Änderungen vornahm
- Änderungszeit und Änderungsdatum
- Änderungsgrund

Klassifizierung von Störungen

Fehleinschätzungen von Störungen können fatale Auswirkung nach sich tragen: Verzögerungen in Störungsbeseitigung können zu erheblichen Qualitäts- und Produktionseinbußen führen, sowohl beim Kunden als auch beim IT-Unternehmen.

Prozess der Klassifizierung soll die Ursache für die Störung identifizieren und später entsprechende Lösungsaktionen einleiten.

Abgleich mit Problemen und Bekannten Fehlern ist notwendig: vielleicht wurde die Störung schon mal behoben oder es existiert ein Work-around. Dabei gelten die Software-Experten-Systeme als ideale Helfer und werden zur Klassifizierung von Störungen eingesetzt.

Beziehungen zwischen Störung, Problem, Bekannter Fehler und RFC:

Ausfall, Fehler -> Störung -> Problem -> Known Error (Work-around existiert) -> RFC -> Lösung

Klassifizierung leistet folgende Hilfe bei der Behandlung von Störungen

- Beste Spezialistengruppe zur Lösung der Störung bestimmt
- Punkte identifiziert, wo Klärungsbedarf besteht
- Erkennung von fehlenden Informationen

Bei Problemen:

- Umfassende Untersuchung
- Erstellung eines Problem-Records
- Einschaltung des Problem Managements bei schweren Störungen
- Nicht alle Probleme können gelöst werden (Störung abgeschlossen, Problem existiert weiter)

Priorisierung von Störungen

Wichtiger Aspekt in der Behandlung von Störungen ist ihre Priorisierung. Durch die Priorisierung von Störungen wird bei deren Behandlung indirekt nicht nur die Reihenfolge in weiteren Support Leveln, sondern auch der Lösungsaufwand bestimmt.

Priorität von Störungen ist definiert als Summe von Dringlichkeit und Auswirkung.

- Dringlichkeit
 - Maß für Schnelligkeit, mit der eine Störung behoben werden muss.
- Auswirkung
 - Ausmaß einer Störung, wer und was ist betroffen.

Sinnvollerweise werden Kriterien zur Bestimmung von Auswirkung und Dringlichkeit einer Störung gemeinsam mit dem Kunden erarbeitet und abgestimmt. Auf diese Weise ist sichergestellt, dass die Einstufung tatsächlich auch den geschäftlichen Prioritäten des Kunden gerecht wird.

Es sollten auch mögliche Folgen für das eigene IT-Unternehmen berücksichtigt werden wie z.B. Folgekosten, rechtliche Konsequenzen, Gefahr für Mitarbeiter oder auch Imageverlust.

Bei der Priorisierung kann auch eine Prognose abgegeben werden, wie sich die Störung auswirken könnte.

Lösungssuche durch Analyse und Diagnose (und Wiederherstellung)

Wird von einem Support Team durchgeführt. Die Auswirkungen der zu behandelnden Störung auf den Kunden sollen minimal sein. Aus diesem Grund sollte möglichst schnell dem Service Desk ein Vorschlag zum Work-around gemacht werden, fall möglich. Ansonsten muss folgendes sichergestellt werden:

- Status der Störung und Historie sind aktuell
- Kunde wird über den Verlauf der Störungsbehandlung informiert

Die vorliegende Störung soll mit Bekannten Fehlern, Problemen, Lösungen, geplanten Änderungen und Wissensbasis abgeglichen werden. Eventuell kann Service Desk aufgefordert werden die Störungsklassifikation und Priorisierung zu evaluieren

Für die Beseitigung der Störung werden zuerst alle störungsbezogene Informationen gesammelt und analysiert. Alle durchgeführten Aktionen zur Störungsbeseitigung werden dokumentiert:

- Lösungsweg
- Hinzugefügte/aktualisierte Klassifizierung
- Aktualisierung aller zugehöriger Störungen
- Zeitaufwand

Dieser Schritt kann auch ein iterativer Prozess sein, an dem verschiedene Spezialisten über längeren Raum beteiligt werden und sich abwechseln, auch externe.

Service Desk kann die Lösungssuche für Störungsursachen auch an das Problem Management delegieren.

Abschluss von Störungsvorgängen

Vorgenommene Überprüfungen, ob

- Kunde die Lösung bestätigt hat und zufrieden
- Lösungsweg im Incident Record knapp und lesbar
- Zeitaufwand im Incident Record eingetragen
- Person, Zeit und Datum des Abschluss vorhanden

Zuständigkeit, Überwachung, Nachverfolgung und Beauskunftung

Folgende Aktivitäten helfen, dass Störungen so schnell wie möglich, innerhalb des vereinbarten Zeitrahmens, gelöst werden

- Alle geöffnete Störungen überwachen, nachverfolgen
- Einschaltung des Problem Managements bei schweren Störungen
- Störungsbeseitigung delegieren
- Kunden über aktuellen Stand von Störungsbehandlung informieren
- Ähnliche Störungen suchen

Vorteile des Incident Managements

- Erhöhung allgemeiner Leistungsfähigkeit der IT-Infrastruktur
- Schnellere Bearbeitung von Störungen
- Mitarbeiter werden effektiver eingesetzt
- Seltener Verluste oder Falscheinschätzungen von Störungen
- Kunden fühlen sich mit zentraler Anlaufstelle (Service Desk) für beliebige Störungen besser betreut
- Verbesserte Management Informationen zur Erhöhung der Service Qualität

Literaturquellen:

[1] Alfred Olbrich; ITIL kompakt und verständlich; Vieweg; 2004

[2] Jochen Sommer; IT-Servicemanagement mit ITIL und MOF; mitp; 2004

[3] Best Practice for Service Support; Office of Government Commerce; 2000