HANSER

Leseprobe

Christian Wischki, Lutz Fröhlich

ITIL® & ISO/IEC 20000 für Oracle Datenbanken

Praxisleitfaden für die Einführung und den Betrieb

ISBN: 978-3-446-41978-0

Weitere Informationen oder Bestellungen unter

http://www.hanser.de/978-3-446-41978-0

sowie im Buchhandel.

4

4 Das Incident Management

4.1 Das Incident Management unter ITIL

Der Incident-Management-Prozess zählt für den Anwender zu den sichtbarsten Prozessen einer IT-Organisation. In diesem Prozess werden Störungen möglichst effektiv behoben, sodass der Service, wie im SLA (Service Level Agreement) vereinbart, wieder gewährleistet ist. Dazu ist es notwendig, Prozeduren für die Aufzeichnung, die Priorisierung, das Management der Auswirkungen, die Auswirkungsanalysen für das Business, die Klassifizierung, die Aktualisierung, die Eskalation, die Lösung und das formelle Schließen von Incidents zu entwickeln, zu definieren und einzuführen. Um jedoch einen Incident-Management-Prozess effektiv entwickeln und ausführen zu können, muss vorab festgelegt sein, was eine Störung (Incident) überhaupt ist:

- **Incident:** Ereignis, Störung oder Zwischenfall, den eine nicht geplante betriebsbedingte Aktion (Maintenance), eine tatsächliche oder potenzielle Unterbrechung oder auch eine Minderung des im SLA vereinbarten Service verursacht.
- **Service Request:** eine Anfrage des Kunden, kein Incident im eigentlichen Sinne, da der im SLA vereinbarte Service nicht gestört ist. Klassische Service Requests stellen Anfragen bzgl. Service-Erweiterung (neue Funktionen, zusätzlichen Support etc.), eine Dokumentation oder Unterstützung der Anwender dar.
- **Complaint:** Kundenbeschwerde, ebenfalls *kein* Incident im engeren Sinn, da auch hier der im SLA vereinbarte Service nicht gestört ist. Eine Beschwerde führt in der Praxis oft zu einem Service Request, ist jedoch zunächst kein solcher.

Entscheidend für den Start des Incident-Management-Prozesses ist, dass eine Störungsmeldung – egal ob sie von einem Monitoring-System oder von einem Anwender stammt – eindeutig identifizierbar ist und dass es sich wirklich um eine Störung handelt. Vor allem bei eingehenden Anwendermeldungen ist häufig der Unterschied zwischen Incident, Service Request und Complaint nicht erkennbar, wenn das entsprechende SLA dem Incident Management nicht bekannt ist.

Praxistipp

Grundlage für die Definition einer Störung ist immer das jeweilige SLA – nicht der nach Meinung des Anwenders zu erbringende Service der IT-Organisation. Im SLA sind die zu erbringenden Services und deren Levels definiert. Nur wenn diese nicht erfüllt sind, liegt ein Incident vor.

4.1.1 Der Incident-Management-Prozess

Abbildung 4.1 zeigt einen Incident-Management-Prozess, bei dem der Kunde bzw. das Business stets über den gesamten Zyklus einer berichteten Störung (oder auch einer Service-Anfrage) hinweg informiert und im Falle einer Minderung des vereinbarten Service-Levels proaktiv benachrichtigt und über die vereinbarten eingeleiteten Maßnahmen informiert wird.

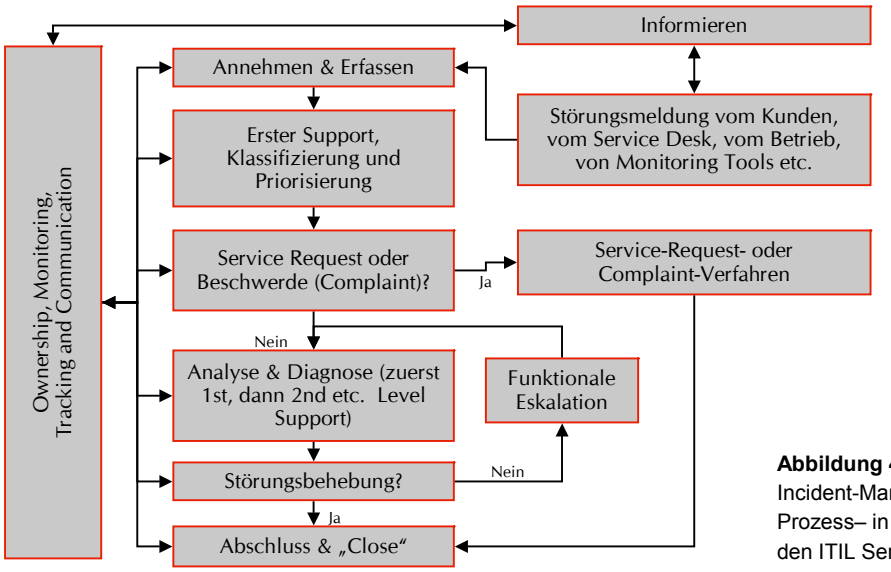

Abbildung 4.1
Incident-Management-Prozess– in Anlehnung an den ITIL Service Support

Identifikation von Störungen

Störungen werden in der Praxis entweder vom Anwender identifiziert und gemeldet – was allerdings für die IT kein gutes Zeugnis darstellt – oder durch ein Monitoring-System der IT, was auf eine effektive Funktionsweise der IT hindeutet.

Erfassung von Störungen

Alle Incidents müssen aufgezeichnet werden. Das Incident Management überprüft, ob die Störungsinformationen – egal, ob automatisiert oder manuell – auch wirklich Störungen darstellen. Sollten sie sich als Störung herausstellen, werden sie erfasst, was in der Praxis mittels eines Ticketing-Tools erledigt wird. In der Regel gilt: pro Incident ein Ticket.

Bei der Störungserfassung ist großer Wert darauf zu legen, dass die Störungsinformationen stets vollständig erfasst sind – und vor allem ist auf das entsprechende Configuration Item (CI – siehe Kapitel 10) zu referenzieren, was eine Verbindung zwischen Ticketing-Tool und Configuration Management Database (CMDB – siehe Kapitel 10) erfordert. Anschließend folgt die Klassifizierung und Priorisierung des Incidents.

Klassifizierung und Priorisierung

Bei der Klassifizierung von Incidents unterscheidet man grundsätzlich zwischen normalen und großen (major) Incidents. Beim Major Incident sind in der Regel sehr viele Anwender und/oder IT-Services betroffen, was dann eine entsprechende Priorisierung des Incidents zur Folge hat. Die Priorität eines Incidents ergibt sich stets aus der Kombination von Auswirkung (z.B. Anzahl der betroffenen Anwender) und Dringlichkeit (z.B. produktives System oder Testsystem), wobei Major Incidents stets nicht nur eine hohe Priorität haben, sondern auch vor allen anderen Incidents absolut vorrangig zu bearbeiten sind.

Praxistipp

Major Incidents sollten stets über einen eigenen Prozess klassifiziert und gehandhabt werden, da sie fast immer Störungen darstellen, die besonders große Auswirkungen auf die Kunden und das Business zur Folge haben. Für normale Incidents wird in der Regel eine dreistufige Priorisierung verwenden – hoch, mittel und niedrig.

Meist unterhält eine IT-Service-Organisation jedoch mehrere SLAs und auch mehrere IT-Services. Hier sollte man die definierte Priorisierungsmatrix um eine weitere Dimension der verschiedenen SLAs erweitern, da in jedem SLA normalerweise andere Reaktions-, Lösungs- und Wiederherstellungszeiten sowie ggf. zusätzliche Vertragsstrafen vereinbart sind, was vor allem bei größeren Unternehmen und externen IT-Dienstleistern der Fall ist.

Diagnose und Analyse

Anschließend erfolgt eine Erstdiagnose und -analyse der Störung, doch nur in der dafür notwendigen Tiefe, um die Störung zu beheben. Probate Mittel sind:

- Eine Knowledge-Database oder Known-Error-Database (Wissensdatenbank). In dieser sind unter anderem bekannte Fehler sowie deren Behebungen oder Workarounds hinterlegt.
- Eine Configuration Management Database

Sollte im First-Level-Support die Störung nicht behoben werden können, findet eine entsprechende Eskalation – eine funktionelle Eskalation – in den nächsthöheren Support-Level statt. Dieser versucht dann, die Störung zu beheben, oder eskaliert sie in den für ihn nächsthöheren Level. Das Ganze geht so lange, bis die Störung behoben ist.

Das Gegenteil einer funktionellen Eskalation ist die hierarchische Eskalation – beispielsweise zum Incident Manager, der für den gesamten Incident-Prozess verantwortlich ist. Dieser Weg wird in der Praxis meistens nur bei Beschwerden seitens des Anwenders beschritten oder wenn ein Major Incident vorliegt.

Praxistipp

Bei Major Incidents und normalen Incidents mit einer hohen Priorität sollten in jedem Fall mittels eines Problem-Tickets, welches durch das Incident Management eröffnet werden sollte, eine Root-Cause-Analyse (Ursachenanalyse) seitens des Problem Managements initiiert werden, um so sicherzustellen, dass die Ursache der Störung identifiziert und auch nachhaltig behoben wird.

Störungsbehebung und Abschluss

Ist die Lösung bekannt, wird die Störung durch das Incident Management behoben und der Störungsmelder entsprechend informiert. Erst wenn der Anwender oder das meldende System bestätigt, dass die Störung behoben ist, wird sie vom Incident Management geschlossen – und nicht, wenn die IT-Organisation der Meinung ist, dass die Störung behoben ist.

4.2 Das Incident Management unter ISO20000

Die ISO20000 Norm ist hier konkreter, indem sie die allgemeinen Anforderungen des Incident-Managements unter ITIL präzisiert. Diese Anforderungen sind in der ISO-20000-Norm (Teil 1) wie folgt beschrieben:

- Alle Incidents müssen aufgezeichnet werden.
- Es müssen Prozeduren definiert und eingeführt sein, mit deren Hilfe sich die Auswirkungen von Störungen handhaben lassen.
- Für folgende Incidents müssen Prozeduren definiert sein:
  - Aufzeichnen von Incidents
  - Priorisierung von Incidents
  - Businessauswirkungsanalysen von Incidents
  - Klassifizierung von Incidents
  - Updating von Incidents
  - Eskalation von Incidents
  - Lösung von Incidents
  - Formelle Schließung von Incidents
- Der Kunde muss über den gesamten Zyklus seiner berichteten Störung oder seiner Serviceanfrage hinweg informiert werden; im Falle einer Minderung des vereinbarten Service Levels muss der Kunde pro-aktiv seitens des Service Providers alarmiert und über die vereinbarten eingeleiteten Maßnahmen informiert werden.
- Alle involvierten Personen innerhalb des Incident Managements müssen Zugriff auf alle hierfür relevanten Information besitzen, wie beispielsweise auf Known Errors, Problemlösungen, Workarounds und die CMDB.
- Major Incidents müssen mittels eines eigens hierfür definierten Prozesses entsprechend klassifiziert und gehandhabt werden.

Ziel ist es, dass der vereinbarte Servicelevel für das Business im Störungsfall so schnell wie möglich wiederhergestellt oder Letzterer im Falle eines Service Requests seitens des Service Providers auch qualitätsgesichert bearbeitet wird.

4.3 Das Incident Management für Oracle Datenbank Services

Der Incident-Management-Prozess ist für die Kunden eines Oracle Datenbank Service einer der sichtbarsten Prozesse. Das grundsätzliche Ziel dieses Prozesses ist die möglichst effektive Störungsbehebung, so dass der Oracle Datenbank Service – wie er im SLA definiert ist – so schnell wie möglich wieder gewährleistet ist

Das Incident Management kann in der Praxis organisatorisch unterschiedlich aufgesetzt sein. Dabei spielt es keine Rolle, ob Aufgaben oder Prozesse durch interne oder externe Leistungen eines Unternehmens abgedeckt werden. Der Incident-Management-Prozess selbst sollte jedoch mit Fokus auf ITIL, wie in Abbildung 4.1 dargestellt, aufgesetzt werden.

Hinweis

Um eine saubere Abgrenzung zwischen Incident und Problem nach ITIL und ISO20000 zu gewährleisten, sprechen wir in diesem Zusammenhang stets von einem Incident, einer Störung oder einem Störfall und vermeiden den Begriff „Problem“, auch wenn der Anwender zum Beispiel bei einer Störungsmeldung häufig von einem Problem spricht.

Ein Incident in Zusammenhang mit einer Oracle-Datenbank ist eine aktuelle oder auch potenzielle Störung, die den Datenbankservice – so wie dieser im SLA definiert und vereinbart ist – in irgendeiner Form direkt oder indirekt beeinträchtigt. Diese Definition ist recht weit gefasst, da sie zum Beispiel auch Probleme auf dem Datenbank-Client, beispielsweise mit einem JDBC-Treiber, einschließt. Eine indirekte Beeinflussung kann beispielsweise auch ein Umstand sein, der keine sofortige Störung verursacht, aus dem heraus aber eine zukünftige Störung erwachsen kann. In der Praxis hat sich gezeigt, dass die Komplexität des Oracle-Datenbank-Umfelds eine solch umfassende Definition erforderlich macht. Dazu ein Beispiel:

Beispiel

Einer von zwanzig Benutzern meldet die Störung, dass eine Verbindung von seinem Client zur Datenbank mit dem folgenden Fehler abgewiesen wird:

ERROR:
ORA-00604: error occurred at recursive SQL level 1
ORA-12705: Cannot access NLS data files or invalid environment specified

Diese Störung sieht auf den ersten Blick nicht nach einer Datenbankstörung, sondern nach einer Client-Störung aus, da die anderen neunzehn Clients ja problemlos auf die Datenbank zugreifen können. Eine Analyse ergibt, dass der Client eine andere Language-Einstellung verwendet. Die Ursache ist, dass infolge einer unsauberen Installation der Oracle-Software die Message-Datei für seine Spracheinstellung auf dem Datenbankserver fehlt.

Die Identifikation von Störungen kann auf verschiedene Art und Weise erfolgen. Die häufigsten Formen in der Praxis sind:

- *Identifikation durch den Anwender:* Der Anwender meldet die Störung dem First Level-Support.
- *Identifikation durch das Monitoring*: Das Monitoring sendet eine Warnung oder einen Alarm über eine aktuelle oder potenzielle Störung.

Sie erkennen bereits den Unterschied. Während bei der Identifikation durch den Anwender bereits eine Auswirkung auf den normalen Betrieb vorliegt, identifiziert das Monitoring darüber hinaus potenzielle Störungen und/oder auch ggf. Probleme zu einem Zeitpunkt, da die Datenbank aus Sicht des Anwenders noch ohne Störungen läuft. (An dieser Stelle wird auch deutlich, weshalb der Begriff des Incidents so weit gefasst werden muss.)

Das Incident Management wird von Oracle seit der Version 11g durch das *Automatic Diagnostic Repository (ADR)* wesentlich besser unterstützt. Das ADR ist ein Repository auf Datei-Ebene, das Log-, Trace- und Alert-Dateien enthält. Im Falle eines Incidents führt Oracle hier die folgenden Operationen durch:

- Einen Eintrag in die Alert-Datei erstellen.
- Eine Incident-Nachricht an den Enterprise Manager senden.
- Sammeln von Diagnostic-Daten und Zusammenfassung in Incident Dumps.
- Jeder Incident sowie die zugehörigen Dateien im ADR werden mit einer eindeutigen ID versehen.
- Alle Informationen in einem Unterverzeichnis des ADR speichern.

Somit ist jede Störung eindeutig nachvollziehbar und kann beispielsweise auch im Enterprise Manager über die Support Workbench verwaltet werden.

Der Major Incident

Um eine ISO20000-Konformität zu gewährleisten, muss innerhalb des Incident Managements auch zwingend ein dedizierter Incident-Prozess für sogenannte Major Incidents entwickelt werden bzw. vorhanden sein. Doch was stellt überhaupt einen Major Incident für Oracle Datenbankservices dar?

Ein Major Incident liegt im Grunde immer dann vor, wenn weite oder wichtige Teile des Service – wie im SLA vereinbart – nicht mehr zur Verfügung stehen, d.h., beispielsweise wenn Incidents an SPOFs (Single Point of Failures) vorliegen oder ein Incident eine VBF (Vitale Business Function) erheblich beeinträchtigt. Im Falle von Oracle Datenbank Services kann man grundsätzlich festlegen, dass ein Major Incident immer dann vorliegt, wenn etwa aufgrund von aktuellen oder zukünftigen Datenbankstörungen

- einzelne oder mehrere Datenbanken nicht mehr verfügbar sind;
- einzelne oder mehrere für das Business relevante Middlewares oder Applikationen auf die Datenbank nicht mehr zugreifen können oder diese dadurch in ihrer Funktionalität signifikant beeinträchtigt sind.

Im Grunde wird der Major-Incident-Prozess in der Praxis weitgehend analog zu den „normalen“ Incident-Prozessen behandelt – mit dem Unterschied, dass u.a.

- man auf ihn erheblich schneller reagieren muss;
- er priorisiert bearbeitet wird;
- hier zwingend auch ein Problem-Ticket für eine Root-Cause-Analyse eröffnet werden muss (ggf. auch nachgelagert, wenn dies für die Störungsbehebung unerheblich ist);
- das pro-aktive Problem Management auch alle anderen Datenbanken in Bezug auf die identifizierte Ursache prüft und diese Fehlerquelle dann bei ihnen auch zeitnah pro-aktiv eliminiert.

Praxistipp

Wenn ein Major Incident vorliegt, sollte er seitens des Incident Management oder des Service Desks sowohl an die Kunden als auch an die Mitarbeiter des Oracle Datenbank Service immer pro-aktiv kommuniziert werden. Außerdem sollten in der Zeit, bis der Major Incident behoben worden ist, keine weiteren Störungen seitens des Incident Managements bzw. des Service Desks erfasst werden, da in diesem Fall die Wahrscheinlichkeit groß ist, dass diese Störungen auch mit der Behebung des Major Incidents behoben werden können. Sobald der Major Incident dann behoben ist, muss seitens des Incident Managements oder des Service Desks – sowohl an die Kunden als auch an die Mitarbeiter des Oracle Datenbank Service – pro-aktiv kommuniziert werden, dass der Major Incident jetzt behoben wurde und der Oracle Datenbank Service wieder zur Verfügung steht.

4.3.1 Strukturen des Incident Managements für Oracle Datenbank Services

In der Praxis hat sich für die meisten Oracle Datenbank Services ein dreistufiges Incident Management bzw. eine dreistufige Support-Level-Struktur innerhalb des Incident Managements bewährt, was anhand der Abbildung 4.2 (nächste Seite) verdeutlicht wird.

4.3.1.1 Der First Level Support

Die erste Stufe – auch First-Level-Support genannt – nimmt grundsätzlich alle Störungsmeldungen entgegen. Hier werden die Störungsmeldungen vollständig aufgenommen, identifiziert, klassifiziert und priorisiert sowie – wenn möglich – behoben.

Praxistipps

Mit der Aufnahme des Incidents durch den First Level Support erfolgt auch die Erstklassifizierung und -priorisierung. Der Name sagt bereits, dass eine spätere Neu-Klassifizierung sowie Neu-Priorisierung durchaus möglich ist. Dabei ist es jedoch essenziell, dass die Klassifizierung stets aus Sicht des Business und nicht aus technischer Sicht erfolgt. Es ist also eher unwichtig, ob es sich um einen schweren Bug aus technischer Sicht handelt – entscheidend ist immer, welchen Impact er auf das Business verursacht.

Für eine schnelle Störungsanalyse und Behebung ist es auch zwingend erforderlich, dass sowohl alle erforderlichen Störungsinformationen vollständig vorliegen bzw. aufgenommen werden als auch alle Informationen in der CMDB (Configuration Management Database),

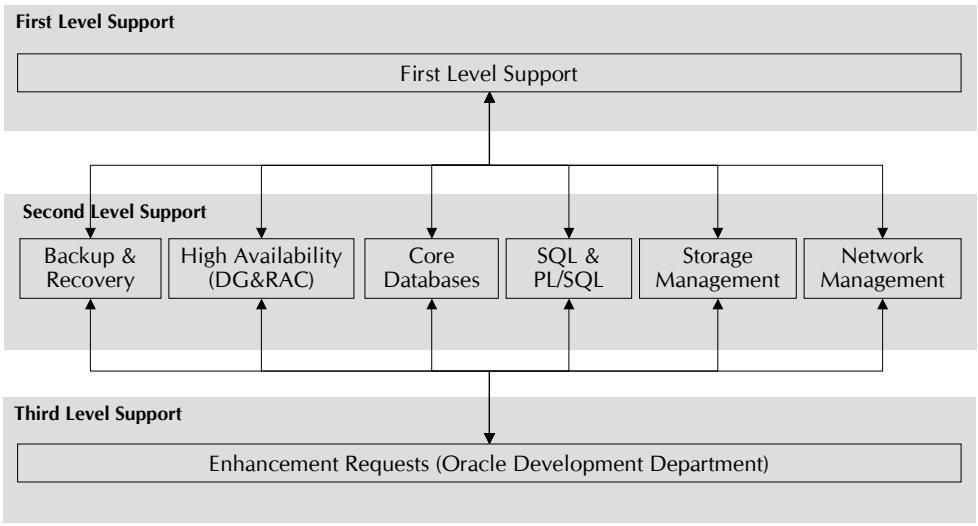

Abbildung 4.2 Eine in der Praxis bewährte Incident Management Support-Level-Struktur für Oracle Datenbank Services

aktuell und vollständig vorhanden sind, da eine zielführende Störungsanalyse und erfolgreiche Störungsbehebung nur basierend auf den realen Parametern und Konfigurationseinstellungen der jeweiligen Datenbanken möglich ist.

Der First Level Support spielt in der Praxis eine bedeutende Rolle bei der Aufnahme von Störungsmeldungen. Weshalb ist diese zentrale Stelle so wichtig? Der in der Regel vom Service Desk durchgeführte First Level Support kann beispielsweise bereits auf Grundlage einer Störungsmeldung feststellen, ob es sich um ein bekanntes Problem (Known Error) handelt. In diesem Fall kann er direkt die Lösung oder einen Workaround zur Beseitigung der Störung liefern. Dies ist natürlich nur möglich, wenn alle Störungsmeldungen an diese zentrale Stelle gehen und der Bearbeiter Zugriff auf die Datenbank der bekannten Probleme (Knowledge DB bzw. KnownError-DB) hat.

Praxistipp

Im Gegensatz zu IT-Services, welche dem Business gegenüber fungieren, stellt der Oracle Datenbank Service im Grunde einen IT-Service der IT für die IT dar, d.h. die Kunden dieses Services, welche u.a. auch Störungen melden, stellen in der Praxis meistens eine wesentlich kleinere Menge dar als die Anzahl der Endanwender. Die Kunden eines Datenbankservice sind in der Regel Applikationen und Middlewares, welche auf den Oracle Datenbank Service zugreifen. Aus diesem Grund sollte bereits die Besetzung des First-Level-Supports für einen Oracle Datenbankservice immer durch qualifizierte DBAs erfolgen, da in diesem Bereich nicht nur die richtige Verteilung oder Weiterreichung von Störungen an die nachgelagerten Supporteinheiten im Fokus steht, sondern – vor allem – auch die Störungsbehebung. Ziel des First-Level-Supports eines Oracle Datenbank Service sollte sein, mehr als 80% der eingehenden Incidents beheben zu können, ohne eine funktionale Eskalation an den Second-Level-Support durchführen zu müssen.

Sollte eine Behebung der Störung in dieser Ebene nicht möglich sein, so wird die Störung vom First-Level-Support an die hierfür fachlich zuständige zweite Stufe des Incident Management – den Second-Level-Support – eskaliert.

Praxistipp

Global aufgestellte Unternehmen sollten den First-Level-Support ebenfalls global aufsetzen. Wenn weltweit auf eine Datenbank zugegriffen wird, ist ein globales Incident und Problem Management zwingend erforderlich.

4.3.1.2 Der Second-Level-Support

Die zweite Stufe – auch Second-Level-Support genannt – besteht im Grunde aus verschiedenen Spezialistengruppen, wie beispielsweise der High-Availability-Gruppe, der Backup-und-Recovery-Gruppe etc. Die Aufgabe des Second-Level-Supports besteht wie die im First Level Incident Management darin, aktuelle oder potenzielle Störungen so schnell wie möglich zu beheben. Sollte eine Behebung der Störung ohne entsprechende Ursachenanalyse jedoch nicht möglich sein, wird an dieser Stelle ein Problem-Ticket eröffnet, welches den re-aktiven Teil des Problem Managements aktiviert.

Das re-aktive Problem Management führt nun in der Regel eine sogenannte „Root Cause Analyse“ durch, ermittelt dadurch die Ursache und stellt dem Incident Management dann eine entsprechende Lösung oder einen Workaround zur Behebung der Störung zur Verfügung, die seitens des Incident Managements geplant und durchgeführt wird.

Praxistipp

Der Incident kann geschlossen werden, sobald der Oracle Datenbank Service – wie im SLA vereinbart – wieder zur Verfügung steht. Jedoch kann es auch durchaus der Fall sein, dass das entsprechende Problem-Ticket weiterhin noch offen bleiben muss, da zwar die Störung behoben ist, jedoch das Problem hinter der Störung vielleicht noch nicht nahhaltig behoben wurde oder auch die Möglichkeit besteht, dass andere Datenbanken von der Störung auch betroffen sein können. In diesem Fall muss dann auch ggf. der pro-aktive Teil des Problem Managements aktiv werden.

In der Regel sollten diese Spezialistengruppen im Second-Level-Support des Incident Managements und dem re-aktiven Problem-Management alle auftretenden Störungen beheben können, die keine Änderungen an der Herstellersoftware, der Oracle Datenbanksoftware selbst also, voraussetzen. Sollte dies jedoch nicht der Fall sein oder die Störungsbehebung nur mittels Änderungen an der Herstellersoftware möglich sein, wird die Störung anschließend an die dritte Stufe des Incident Managements eskaliert.

Praxistipp

Der Second-Level-Support sollte im Bereich von Oracle Datenbank Services in die Fachbereiche Backup/Recovery, High Availability (DataGuard / RAC), Core-DB, SQL & PL/SQL und Storage Management untergliedert werden. Selbstverständlich lassen sich die Second-Level-Gruppen bei Bedarf auch erweitern.

4.3.1.3 Der Third Level Support

Die dritte Stufe – auch Third-Level-Support genannt – wird in der Praxis eigentlich immer an den Hersteller, in diesem Fall an die Firma Oracle mittels entsprechender Supportverträge ausgelagert, da in der Regel nur sie in der Lage ist, Änderungen an der Oracle Datenbanksoftware vorzunehmen bzw. qualitätsgesichert durchzuführen.

Praxistipp

Laut Supportvertrag ist Oracle jedoch nicht verpflichtet, einen Bugfix zur Verfügung zu stellen, wenn der Bug in einer höheren verfügbaren Version beseitigt ist. Außerdem wird Oracle immer zuerst den Bugfix für die höhere Version zur Verfügung stellen. Es gibt jedoch Situationen, in denen ein Upgrade der Datenbank nicht möglich ist. Dann muss mit Oracle über die Möglichkeit eines Backports verhandelt werden.

Oracle bietet hierfür als Schnittstelle die Webseite „My Oracle Support“ (früher Metalink) an: http://support.oracle.com (siehe Abbildung 4.3). Hier kann jeder Kunde, der über einen Support-Vertrag und somit über eine „Customer Identification Number (CID)“ verfügt, einen Service Request (früher Technical Assistant Request, kurz TAR) eröffnen.

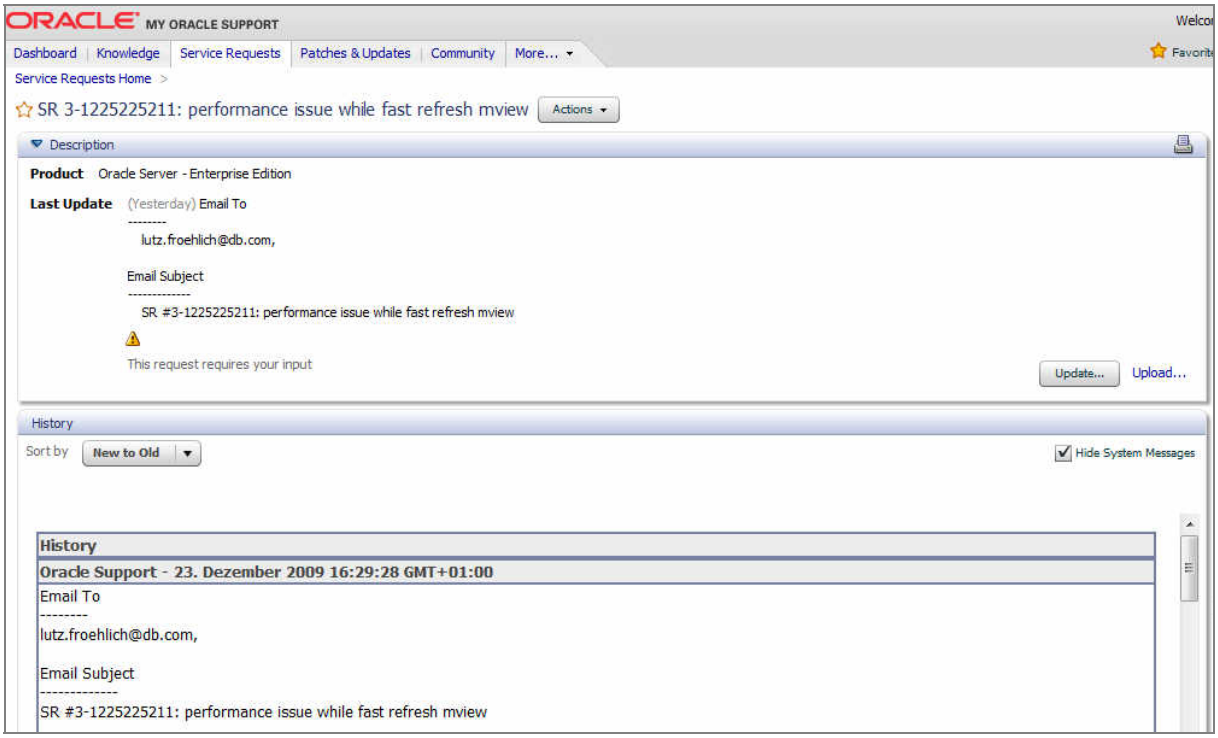

Abbildung 4.3 Die „My Oracle Support“-Webseite

Praxistipp

Oracle stellt auch den „Configuration Manager“ zur Verfügung. Damit werden die Konfiguration sowie aktuelle Log- und Trace-Dateien zu Oracle Support geladen und stehen bei der Eröffnung eines Service Requests zur Verfügung. Dieses Verfahren beschleunigt die Bearbeitung von Service Requests und schließt Fehler beim Upload von Konfigurations- und Logdateien aus.

Ein Oracle Service Request kennt 4 Klassen, die sich an die Klassifizierung des Incidents anlehnen. So bedeutet beispielsweise „Severity 1“, dass es sich um eine schwere Störung mit erheblichen Einschränkungen für das Business handelt. Auch hier steht die Auswirkung auf das Business immer im Vordergrund, nicht die technische Beurteilung des Schweregrades.

Praxistipps

Service Requests mit „Severity 1“ werden durch Oracle rund um die Uhr nach dem „Follow-the-Sun-Prinzip“ in vier Zeitzonen bearbeitet. Dies bedeutet für den Second-Level-Support, dass ein Ansprechpartner rund um die Uhr zur Verfügung gestellt werden muss. Beachten Sie auch, dass Oracle einen Service Request mit „Severity 1“ nur dann akzeptiert, wenn die entsprechende Auswirkung auf das Business nachgewiesen ist. Halten Sie deshalb die geforderte Business Justification bereit. Die Tatsache, dass sich eine wichtige Produktionsdatenbank nicht mehr starten lässt, reicht für einen Severity 1 Request aus.

Wird seitens Oracle ein Workaround gefunden, mit dem die Datenbank wieder „einsatzfähig“ gemacht werden kann, ohne dass die Ursache hierfür bereits ermittelt wurde, kann der Service Request auf „Severity 2“ herabgestuft werden. Anschließend wird auf beiden Seiten zu normalen Geschäftszeiten an der weiteren Analyse und der Root-Cause-Ermittlung gearbeitet. Die Beseitigung der Störung können beispielsweise folgende Maßnahmen erreichen:

- Einspielen eines Bug Fixes
- Upgrade der Datenbankversion
- Erfüllen eines Enhancement Requests
- Implementierung eines Workarounds

Praxistipp

Beachten Sie beim Herabstufen oder Eröffnen eines Services Requests mit „Severity 2“, dass dieser, abhängig von der Tageszeit, möglicherweise an einen Bearbeiter in einer anderen Zeitzone fällt. Dies verlängert den Gesamtprozess, da die Überschneidung der normalen Geschäftszeiten zwischen Second Level Support und Oracle Support täglich nur wenige Stunden betragen. In solchen Fällen ist es sinnvoll, die Übertragung an einen Bearbeiter in der Europäischen Zeitzone zu beantragen.

So wie eine funktionale Eskalation des Incidents an das nächste Supportlevel erfolgen kann, ist es auch möglich, einen Service Request bei Oracle Support (also innerhalb des Third Level Incident Managements selber) zu eskalieren. Gründe für die Eskalation können beispielsweise folgende sein:

- Die Problemanalyse macht keine Fortschritte innerhalb eines größeren Zeitfensters.
- Die gelieferte Lösung oder der gelieferte Workaround funktioniert nicht, wird nicht akzeptiert oder kann im betrieblichen Umfeld nicht umgesetzt werden.
- Die Aktionspläne sind wenig zielführend oder gehen am Problem vorbei.

Praxistipp

Erstellen Sie zusammen mit dem Oracle Support auch immer eine Art „*Escalation Map“,* in der ein Ansprechpartner oder eine Hotline-Nummer für jede Eskalationsstufe fest vereinbart ist. Im Falle einer Störung ist es wichtig, dass auch die Eskalationen ohne Verzögerungen funktionieren.