



Was wir vorhersagen, soll auch eintreffen!



IT-Operations Analytics (ITOA) - Den IT-Betrieb mit Big-Data Analytics optimieren //

Timo Heise



Einleitung

Unternehmen stehen vor immer größer werdenden Herausforderungen. Im Zuge der Globalisierung herrscht auf internationaler Ebene ein starker Wettbewerb, welcher einen stetigen Veränderungsdruck auf die Unternehmen ausübt. Ständig entwickeln sich auf Kundenseite neue Anforderungen, wodurch die eigenen Produkte und Leistungen kontinuierlich angepasst werden müssen. Um sich den genannten Herausforderungen stellen zu können, müssen die Unternehmen gerade wegen des Kostendrucks neue Geschäftsmodelle erschließen und ihre Prozesse an die neuen Gegebenheiten anpassen und effizienter gestalten. Verändern sich Prozesse oder Geschäftsmodelle von Unternehmen, muss auch die IT-Landschaft entsprechend angepasst werden. Dies bedeutet für den IT-Betrieb, dass die IT-Infrastruktur hochverfügbar, stark skalierbar und flexibel auf Umwelteinflüsse und Veränderungen reagieren muss. Zudem soll der Endanwender möglichst wenig von dem IT-Betrieb spüren – ein reibungsloser und problemfreier Betrieb wird erwartet. Dies ist für den Chief Information Officer (CIO) eine Mammutaufgabe, da auch aktuelle Trendthemen, wie z.B. das Internet der Dinge oder Integration von Cloud-Diensten, nicht zur Komplexitätsreduktion beitragen. Trotz dieser Problematiken stellt die Geschäftsleitung der IT weiterhin Anforderungen, wie beispielsweise Effizienzsteigerung, Kostenreduzierung, Ausbau der Digitalisierung sowie schnelle Bereitstellung neuer und moderner IT-Services. Eine hochflexible und adaptive IT-Infrastruktur soll bei gleichen oder gar sinkenden Betriebskosten agilere Prozesse gewährleisten. Dadurch kann schneller auf Kundenwünsche reagiert werden.

Diesem Problem und weiteren Herausforderungen im IT-Betrieb stellt sich das Konzept IT-Operations Analytics (ITOA). Mithilfe von ITOA besteht die Möglichkeit, aus verschiedenartigen Maschinendaten (bspw. Logdaten) Erkenntnisse zu gewinnen und so zukünftige Ereignisse vorherzusagen. Auf diese Weise können Daten aus dem IT-Betrieb genutzt werden, um die Servicequalität zu verbessern, die Verfügbarkeit der IT-Infrastruktur zu erhöhen und Ausfälle von Hardwarekomponenten zu prognostizieren.

Warum IT-Operations Analytics (ITOA)?

Hohe Kosten durch Ausfälle oder Fehlverhalten

Fällt die IT-Infrastruktur eines Unternehmens aus, betrifft dies alle digitalen Prozesse inkl. der vernetzten Produktion, weswegen solch ein Ausfall zu enormen Kosten führen kann. Laut des Marktforschungsunternehmens Gartner kostet ein IT-Systemausfall im Durchschnitt 5.600 USD in der Minute. In drei Stunden summieren sich die Kosten somit auf über eine Million Dollar. Auch die Studie „Masters of Machines III - Mitigating the impact of critical IT events“ des Analystenhauses Quocirca bestätigt die Untersuchungen von Gartner. Im Rahmen der Studie wurde aufgedeckt, dass Ausfälle und Fehlfunktionen ein deutsches Unternehmen durchschnittlich 112.415€ kosten. Diese Critical Incident Events (CIE) treten im Schnitt dreimal monatlich auf und verursachen somit Schäden in Höhe von ca. 4 Millionen Euro jährlich.¹

¹ <https://www.it-daily.net/analysen/13658-kritische-it-ereignisse-millionenkosten-fuer-europaeische-unternehmen-studie>



Schädigung der Unternehmensreputation bei Systemausfällen oder Fehlverhalten

Fällt ein IT-System aus oder ist es gestört kann dies eine negative Reputation des Unternehmens zur Folge haben. Können angebotene Services des Unternehmens in dieser Zeit durch die Kunden nicht genutzt werden, leidet schnell das Image darunter. Dies betrifft z.B. besonders die Telekommunikationsbranche, den Handel sowie den Finanzsektor.

Lange Fehlerbehebungszeiten und Ursachenforschung

Tritt ein Fehler im IT-System auf, dauert es mitunter sehr lange bis der zuständige Bearbeiter identifiziert ist. Tickets werden von einer Abteilung an die nächste geschickt und niemand fühlt sich zuständig. Dies führt zu längeren Fehlerbehebungszeiten und Unzufriedenheit bei den Anwendern.

Performanceprobleme

Zu bestimmten Tageszeiten, nach Werbeaktionen oder z.B. im Weihnachtsgeschäft treten in der IT Störungen auf und die Performance sinkt aufgrund der hohen Nutzeranzahl der IT-Systeme. Dies kann auch wiederum Unzufriedenheit bei den Anwendern oder schlimmstenfalls Umsatzeinbußen z.B. bei Onlineshops nach sich ziehen, da die Kunden den gewünschten Weihnachtseinkauf nicht tätigen können.

Dies sind nur einige Beispiele dafür, warum über den Einsatz von ITOA-Systemen nachgedacht werden sollte. Die umfassende Verknüpfung der IT-Maschinendaten bietet eine vollständige Transparenz und vereinfacht und beschleunigt die Fehlersuche. Dies kann wiederum zu Kostenreduzierungen und geringeren Bearbeitungszeiten von Störungsmeldungen führen. Neben diesen positiven Aspekten ist besonders hervorzuheben, dass ITOA-Systeme durch die Nutzung von modernen Prognosemethoden drohende Ausfälle und Überlastungen von Systemen vorhersagen können. Hierzu werden statistische Modelle auf die IT-Maschinendaten angewendet und so Systemausfälle verhindert. Folglich kann etwaigen Performanceeinbußen entgegengewirkt und rechtzeitig zusätzliche Ressourcen bereitgestellt werden.

Was ist IT-Operations Analytics (ITOA) genau?

Mit IT-Operations Analytics werden IT-Betriebsdaten mithilfe von Big Data Analytics in Echtzeit ausgewertet, so dass das Ergebnis umgehend und präventiv zur Verbesserung des IT-Betriebes beiträgt. Die Einsatzbereiche lassen sich in drei Sektionen unterteilen: **Suchen, Optimieren und Prognostizieren**.

Jedes ITOA-System bietet eine **Suchmaschine** um die gesammelten Daten zu durchsuchen. Hierfür wird meist eine eigens entwickelte Abfragesprache verwendet. Durch diese Suchengine, die über alle IT-Daten hinweg Auswertungen ermöglicht, ist eine schnellere Problemlösung und Root-Cause Ermittlung gewährleistet.

Mittels moderner Machine-Learning Methoden kann das ITOA-System das Verhalten der IT lernen und bei Abweichungen alarmieren. Zudem kann aus dem gelernten Systemverhalten abgeleitet werden, wann ggfs. weitere Ressourcen zur Verfügung gestellt werden müssen, um Performance bzw. Kapazitätsengpässe zu vermeiden. ITOA kann also auch zur Performance-**Optimierung** eingesetzt werden.

Durch **Prognosemethoden** können ITOA-Systeme zukünftige Systemzustände berechnen und evtl. auftretende Ausfälle vorhersagen. Dies können Fragestellungen sein wie: „Wann wird eine Festplatte bei normalem Systemverhalten keinen freien Speicherplatz mehr haben?“, „Welche Festplatte wird aufgrund der historischen Auswertungen als nächstes ausfallen? (Analyse der SMART-Daten)“, „Wird meine Systemleistung bei einer neuen Werbeaktion in meinem Onlineshop ausreichen?“

Zudem können ITOA-Systeme genutzt werden, um Probleme zielgerichtet den jeweiligen IT-Operations Teams zuzuordnen und diese je nach Impact zu priorisieren. Auch Alarme werden in ITOA-Systemen nur noch bei Abweichungen des Systemverhaltens generiert und nicht anhand festgelegter Schwellwerte - dies führt dazu, dass nur noch bei wirklich wichtigen Incidents alarmiert wird und kurzzeitige Abweichungen vom System ignoriert werden.

Doch welche Daten müssen für welche Ergebnisse herangezogen werden?

Die nachfolgende Grafik veranschaulicht die möglichen Datenquellen im Zusammenhang mit den jeweilig zu erwartenden Ergebnissen im Überblick.



Im ersten Reifegrad eines ITOA-Systems werden verschiedene Logdaten ausgewertet, um die Fehlersuche während des Entwicklungsprozesses zu vereinfachen, ein Reporting zu etablieren und ein IT-übergreifendes Monitoring zu ermöglichen. Das ITOA-System fungiert hier als Single Point of Truth - alle IT-Betriebsdaten werden an einer Stelle zentral gesammelt und auswertbar gemacht. So ist eine End-to-End-Betrachtung der IT möglich.

Im zweiten Schritt der Implementierung werden weitere Quellen angebunden, wie z.B. ein Active Directory oder eine Vulnerability Datenbank. Ist diese Stufe etabliert, kann das ITOA-System als IT-Leitstand genutzt werden und bei der Incident-Bearbeitung unterstützen.

In der letzten Stufe werden Applikationsdaten von z.B. SAP-Systemen eingebunden, das Patch-Management sowie weitere Verzeichnisdienste implementiert. Die führt dazu, dass das ITOA-System auch komplexes Fehlverhalten erkennen und Ausfälle oder Probleme vorhersagen kann.



Wie und wo wird IT-Operations Analytics eingesetzt?

Identifizierung von Problemen 72-mal schneller durch Einsatz von ITOA-Software (30 Minuten vs. 36 Stunden)

Ein Großkonzern hatte zum Ziel die Verfügbarkeit der eigenen IT auf einem sehr hohen Level (99,999%) zu gewährleisten und auftretende Fehler schnellstmöglich zu identifizieren und zu beheben. Eine besondere Herausforderung war hierbei, dass zwar bereits Logdaten gesammelt wurden, jedoch setzen die unterschiedlichen IT-Abteilungen, die weltweit verteilt sind, auch verschiedene Analysetools ein. Das hatte zur Folge, dass sich bei auftretenden schwerwiegenden Problemen die Verantwortlichen der Abteilungen in sog. War rooms zusammenfinden mussten, um eine Problemlösung herbeizuführen. Dies hat zeitweise bis zu zehn hochqualifizierte Mitarbeiter stundenlang gebunden und zu hohen Kosten geführt. Das Unternehmen hat sich daraufhin entschieden, eine ITOA-Software einzuführen, indem die zuvor betriebenen Silos (13 verschiedene Tools) zusammengeführt und somit ein abteilungsübergreifender Blick auf alle Daten ermöglicht wurde. Durch den Einsatz des ITOA-Tools konnten die Daten zentral und abteilungsübergreifend analysiert werden und mittels automatisierter Loganalysen, Predictive Analytics und Guided Troubleshooting konnten Fehler früher erkannt und behoben werden. Insgesamt kann mittels ITOA die Fehleridentifizierung nun 72-mal schneller erfolgen, so dass im Ergebnis auch weniger hochqualifizierte Ressourcen gebunden werden.²

Ende-zu-Ende Transparenz und schnellere Fehlerbehebung mit ITOA

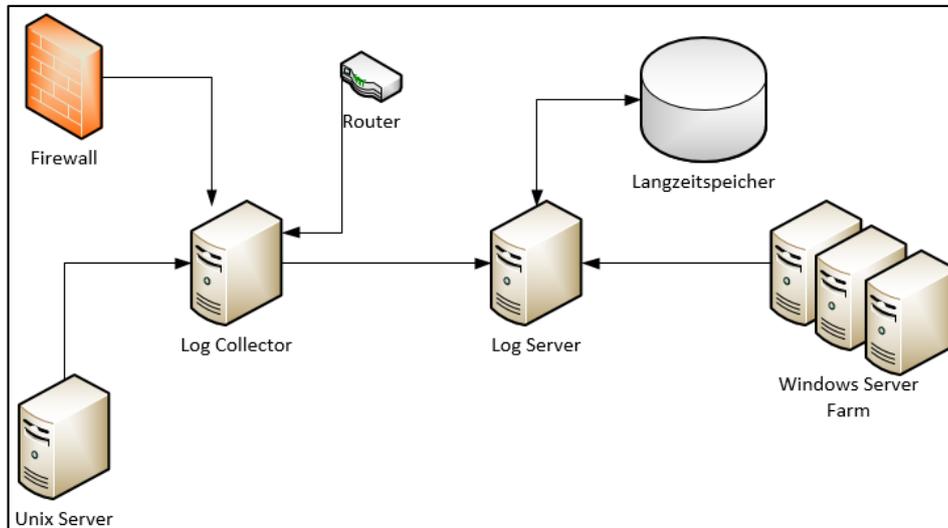
Ein großer Telekommunikationsanbieter stand vor der Herausforderung, dass die Einführung einer neuen Middleware zur Folge hatte, dass durch die bestehende Monitoring Lösung eine sehr große Anzahl von Tickets in Remedy generiert wurde. Das IT-Operations Team war infolgedessen mit der Priorisierung und Bearbeitung überfordert. Auch eine Ende-zu-Ende Transparenz und KPIs für kritische IT-Services war bisher nicht gegeben. Das Unternehmen entschied sich dazu eine ITOA-Lösung einzuführen. Dazu wurden Applikations- und Datenbanklogdaten, Infrastrukturmetriken, Netzwerkmetriken und das Ticketsystem Remedy in das ITOA-System integriert. Durch die Anbindung dieser Quellen und Erstellung statistischer Modell war das ITOA-System in der Lage, die Tickets automatisiert zu priorisieren und den richtigen IT-Operations Teams zuzuweisen. Auch eine Ende-zu-Ende Transparenz in Echtzeit sowie die Abbildung der definierten KPIs für kritische Services konnte mit dem ITOA-System erreicht werden. Das IT-Operations Team konnte somit anhand der Datenauswertungen Trends erkennen und Anomalien aufdecken, woraufhin proaktiv gehandelt und Fehlern und Ausfällen vorgebeugt wurde.³

Wie sehen typische ITOA-Architekturen aus?

Eine ITOA-Architektur muss stark skalierbar sein, viele Schnittstellen bzw. Konnektoren und einen Datenspeicher für historische Analysen aufweisen und Auswertungen in Echtzeit ermöglichen. Neben den genannten Anforderungen kommt dem Punkt Sicherheit eine große Bedeutung zu. Die nachfolgende Grafik zeigt eine allgemeine, stark vereinfachte Architektur eines ITOA-Systems.

² <https://www.hpe.com/h20195/V2/GetPDF.aspx/4AA5-4931ENW.pdf>

³ https://www.splunk.com/en_us/customers/success-stories/vodafone.html



Der in der Abbildung gezeigte Log-Collector sammelt alle Arten von Maschinendaten im jeweiligen Netzsegment und leitet diese an den Log-Server weiter. Dies können, wie auf dem Bild zu sehen, Daten von Firewalls, Servern, Switches, Routern oder andere o.g. Maschinendaten sein. Der Log-Server ist verantwortlich für den Zugriff auf die indizierte Daten und deren Organisation. Für die Auswertung von historischen Daten ist zudem ein Langzeitspeicher an den Log-Server angebunden. Die zentrale Instanz hierbei ist der Log-Server, der die Möglichkeit der Datenanalyse mit sich bringt. Je nach Anforderungen des Kunden und Setup der Infrastruktur kann diese Lösung um beliebig viele Log-Collectoren und Log-Server erweitert werden, um eine hohe Performance und Verfügbarkeit zu gewährleisten.

Welche Hersteller bzw. Produkte gibt es?

Der ITOA-Software Markt ist momentan mit ca. 90 Produkten sehr stark differenziert und es gibt nicht die „beste“ ITOA-Lösung. Vielmehr kommt es auf den Use-Case an. Es gibt z.B. Anbieter wie Nexthink, die sich auf End-User-Analytics spezialisiert haben. Andere Hersteller wie ExtraHop konzentrieren sich auf die Auswertung von Netzwerkdaten. Es gibt aber auch Produkte wie HP Operations Analytics, IBM Operations Analytics oder Splunk, die einen übergreifende Analyse der IT-Betriebsdaten ermöglichen und bereits am Markt etabliert und erprobt sind. Um die passende Lösung zu finden empfiehlt sich eine ausführliche Toolauswahl mit vorher spezifizierten Use-Cases durchzuführen.

Bei einer Toolauswahl, gibt es Kriterien die besonders betrachtet werden sollten. Eine Studie von IDC hat die folgenden wichtigsten Faktoren zur Auswahl von ITOA-Systemen identifiziert⁴:

Die Mindestanforderungen, die ein ITOA-System erfüllen sollte, um in die engere Toolauswahl aufgenommen zu werden, sind nachfolgend aufgelistet.

⁴ IDC, HP Operations Analytics Simplifies and Accelerates IT Service Delivery and Digital Innovation, 2015, S.5&8



- ↗ Einfache Handhabung
- ↗ Kosten
- ↗ Unterstütze Datenquellen
- ↗ Einfach Anpassbarkeit von Dashboard und Reports
- ↗ Qualität der Visualisierungen

Funktionalität

- ↗ Das System muss eine intuitive, moderne und gut strukturierte Benutzeroberfläche besitzen
- ↗ Das Erstellen von Dashboards muss realisierbar sein
- ↗ Ein Alerting bei Überschreiten von Grenzwerten muss eingerichtet werden können
- ↗ Die Auswertung von historischen Daten muss möglich sein
- ↗ Das Durchsuchen von Logdaten muss durchführbar sein
- ↗ Das System muss Analytics Funktionen, wie Machine Learning, unterstützen oder Schnittstellen zu „R“ oder Python anbieten

Sicherheit

- ↗ Eine revisionssichere Speicherung von Logdaten muss möglich sein
- ↗ Die Passwörter müssen verschlüsselt werden
- ↗ Die Kommunikation zwischen Quellsystem und ITOA-System muss verschlüsselt sein
- ↗ Die Kommunikation zwischen dem Anwender des ITOA-Systems und dem ITOA-Systems selbst muss verschlüsselt sein
- ↗ Ein rollenbasiertes Berechtigungskonzept muss umsetzbar sein

Architektur

- ↗ Aktuelle Plattformen wie Windows, Linux und Mac werden unterstützt
- ↗ Der Import von Logdaten / die Anbindung von Logdaten-Quellen muss möglich sein
- ↗ Die Entwicklung von Erweiterungen muss realisierbar sein
- ↗ Die Architektur muss stark skalierbar sein und Big Data-Analytics ermöglichen
- ↗ Die Architektur muss Auswertungen in Echtzeit durchführen können
- ↗ Die Architektur muss gegen einen unberechtigten Zugriff von innen und außen sicher geschützt sein

Chancen und Risiken von ITOA Systemen

Chancen

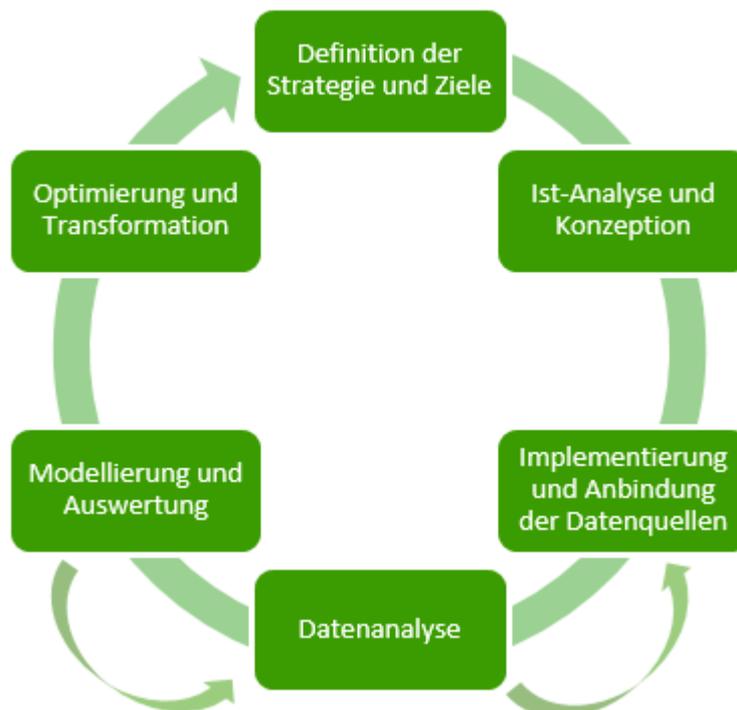
Ein ITOA-System kann die Effizienz der IT steigern, indem es Ressourcen zielgerichtet zuweist. Weiterhin kann durch ein zentral organisiertes ITOA-System die Ursachenanalyse von Fehlern erleichtert werden, da die Suche nicht separat in den einzelnen Fachabteilungen erfolgen muss, sondern in einem zentralen Datenspeicher erfolgen kann. Auch Kapazitätsengpässe können durch die Nutzung intelligenter Algorithmen vorhergesagt und durch die Bereitstellung weiterer Ressourcen vermieden werden. Zudem können mit ITOA-Systemen Einmal-Fragestellungen beantwortet werden, wie z.B. „Was hat ein Herstellerwechsel an Problemen verursacht?“ oder „Was ist bei Fehlern auf eine bestimmte Handlung (z.B. Patch) zurückzuführen?“. ITOA-Systeme können so eine ganzheitliche Sicht auf die IT und ihren derzeitigen Status bieten und somit Transparenz schaffen.

Risiken

In ITOA-Systemen werden große Mengen sicherheitsrelevante Daten, wie z.B. Zugriffsdaten, gespeichert. Außerdem benötigen ITOA-Systeme eine Verbindung zu jedem eingebundenen Netzteilnehmer und Zugriff auf die jeweiligen Daten, was ein Sicherheitsrisiko darstellen kann, wenn das System nicht professionell konfiguriert ist. Dem Thema Sicherheit kommt also eine besondere Bedeutung zu. Es ist sehr wichtig das ITOA-Systeme vor dem Zugriff durch Dritte besonders sorgfältig gesichert werden, da durch Übernahme des Systems weitere angebundene Geräte über die gesamte Infrastruktur hinweg kompromittiert werden können. Ein weiteres Risiko ist, dass die Architektur auf Grund der hohen Frequenz und Menge der Daten überfordert ist und dadurch keine Analysen mehr möglich sind. Auch hohe Kosten können in diesem Kontext eine Rolle spielen, da die Daten rasant wachsen und viele Softwareanbieter im ITOA-Bereich nach der Indizierung der täglich angefallenen Datenmenge abrechnen. Der Datenschutz spielt ebenso eine große Rolle, da mit ITOA-Systemen anhand der Daten auch Benutzeraktivitäten auf Mitarbeitererebene gemessen werden könnten und die erhobenen Maschinendaten auch personenbezogene Daten wie IP-Adressen o.ä. enthalten können.

Wie läuft ein typisches ITOA-Projekt ab?

Aufgrund der Komplexität von ITOA-Systemen ist es sinnvoll bei der Einführung eines solchen Systems nach einem Vorgehensmodell zu verfahren. Die nachfolgende Grafik zeigt einen Ansatz zur Vorgehensweise und wird anschließend erläutert.



Phase 1 - Definition der Strategie und Ziele

Im ersten Schritt des Projektes sollte die Definition der Strategie und Ziele erfolgen. Hier sollten zunächst die aktuellen Probleme und Verbesserungspotenziale im IT-Betrieb erarbeitet und aus diesen Ziele für eine ITOA-Lösung abgeleitet werden. Auch die Stakeholder für ein ITOA-Projekt sollten in dieser Phase identifiziert



werden. Ein ITOA-Projektteam könnte beispielsweise einen ITOA-Architekten, einen Systemadministrator des Kunden, einen Incident-Manager, einen Datenschutzbeauftragten, einen Data Scientist sowie einen Projektleiter umfassen. Nicht jede genannte Rolle muss in allen Phasen im Projekt beteiligt sein. Dies muss entsprechend der Anforderungen in der Strategiebildung definiert werden. Auch eine Risikoanalyse sollte in dieser Phase durchgeführt werden.

Am Ende dieser Phase sollten die folgenden Punkte festgelegt sein:

- Ziele des Projektes / Definition der Problemstellung
- Definition der Stakeholder / Projektbeteiligten
- Definition der Projektrisiken
- Definierter Projektplan

Phase 2 - Ist-Analyse und Konzeption

In der Phase Ist-Analyse und Konzeption wird eine Bestandsaufnahme der aktuellen Infrastruktur des Unternehmens durchgeführt und anschließend auf dieser Grundlage eine Architektur für das ITOA-System entworfen. Neben der Architektur sollte auch ein Berechtigungskonzept definiert werden. Überdies wird in dieser Phase die Auswahl eines ITOA-Tools durchgeführt. Als Grundlage hierfür können die zuvor genannten Mindestanforderungen dienen, die entsprechend verfeinert werden müssen. Im Rahmen der Konzeption ist in dieser Phase auch festzulegen, welche Datenquellen an das ITOA-System angebunden werden sollen. Hierzu sollten der Name, der Datentyp, der Ort und Besitzer, das Format, die Importmethode, das Volumen, die Frequenz und Qualität der Daten sowie der Nutzen der Daten festgelegt werden. Sind eine Architektur mit einem ausgesuchten Tool und die anzubindenden Datenquellen definiert, geht es in die Implementierungsphase.

Am Ende dieser Phase sollten folgende Ergebnisse stehen:

- Überblick über die aktuelle Infrastruktur
- Konzeption einer ITOA-Systemarchitektur
- Definition eines Berechtigungskonzeptes
- Identifizierung und Erläuterung der relevanten Datenquellen

Phase 3 - Implementierung und Anbindung der Datenquellen

Hier wird die konzipierte Architektur aus der zweiten Phase implementiert und die in der Konzeption definierten Quellsysteme angebunden. Bei der Anbindung der Datenquellen sollte für optimale Ergebnisse das erwähnte Reifegradmodell befolgt werden. Die Datenquellen der einzelnen Reifegrade werden im Normalfall nicht in einer Iteration des Vorgehensmodells eingebunden. Vielmehr ist es sinnvoll, zunächst einen Reifegrad nach dem anderen zu durchlaufen, um die Komplexität des Projektes bzw. der Teilprojekte gering zu halten. Es ist also zu empfehlen, das ITOA-Vorgehensmodell in drei Iterationen durchzuführen, um den dritten Reifegrad zu erreichen. Ist jedoch das Ziel des Projektes nur die Schaffung eines Monitorings, ist eine Iteration ausreichend.

In jeder Iteration des Modells sollte in dieser Phase auch die Bereinigung und die Vorbereitung der Daten für eine Analyse enthalten sein. Die angebundenen Datenquellen müssen hier so vorbereitet werden, dass sie in der richtigen Form für erweiterte statistische Auswertungen oder Machine-Learning-Algorithmen vorliegen.

Ist diese Phase beendet sollten folgende Punkte abgearbeitet sein:



- Installation und Konfiguration des ITOA-Systems entsprechend Architekturkonzept und Berechtigungskonzept
- Je nach Zielsetzung und definiertem Reifegrad:
 - Anbindung interner Datenquellen (z.B. Logs von: Betriebssystemen, Switches, Router etc.)
 - Anbindung von Verzeichnisdiensten und Inventardatenbanken
 - Anbindung von Drittsystemen (z.B. Applikationsdaten, Ticketsystem, Monitorings-System etc.)
- Datenvorbereitung für Analyse:
 - Bereinigung der Daten
 - Definieren von Datenfeldern, falls diese nicht vom Tool identifiziert wurden

Phase 4 - Datenanalyse

In diesem Abschnitt werden zunächst die Datenquellen durch die Definition von Abfragen so verarbeitet, dass auf Berichten und Dashboards der aktuelle Systemstatus erkennbar und eine Fehlerüberwachung in Echtzeit möglich ist. Zur Generierung erster Einblicke kann in dieser Phase auch auf vorgefertigte Apps oder Dashboards zurückgegriffen werden, die herstellerspezifische vorgefertigte Abfragen anbieten. Hier wird der erste Mehrwert für das Unternehmen generiert. Durch das Monitoring entsteht eine aktuelle Übersicht über den kompletten IT-Betrieb, das bei einer Vollimplementierung über die komplette IT-Infrastruktur auch End-to-End Monitoring ermöglicht. Diese Phase ist eng gekoppelt mit der vorherigen Phase, der Datenanbindung und -vorbereitung, sodass in der Phase der Datenanalyse möglicherweise festgestellt werden könnte, dass noch weitere Datenquellen für eine aussagekräftige Analyse benötigt werden. In diesem Fall wird in die vorherige Phase zurückgesprungen. Auch die nachfolgende Phase, die Modellierung und Auswertung, ist mit der hier dargestellten Phase vier eng verwoben, da die hier erstellen Analysen die Grundlage für Prognosemodelle bilden.

Im Ergebnis dieser Phase stehen:

- Definition von Suchabfragen zur Beantwortung der Fragestellungen aus der Strategiephase
- Identifikation und Nutzung von Erweiterungen und Apps für schnelle Reports und ersten Überblick
- Einbindung der validierten Suchabfragen in Dashboards und Reports inkl. Visualisierung zum Echtzeit-Monitoring

Phase 5 - Modellierung und Auswertung

In dieser Phase geht es um die Nutzung von Predictive Analytics. Hierzu müssen zunächst ein geeignetes Analysewerkzeug und Analysemethoden identifiziert werden. Im Idealfall bringt eine ITOA-Software diese Funktionalität mit sich, andernfalls können durch die Anbindung oder Nutzung gängiger Programmiersprachen, wie „R“ oder Python, Vorhersagemodelle erstellt werden. Im Anschluss an die Modellierung müssen die Modelle validiert und die Ergebnisse ausgewertet werden. Diese Phase wird je nach Fragestellung beliebig oft wiederholt.

Die Ergebnisse dieser Phase sind:

- Validierte statistische oder Data-Mining Modelle
- Vorhersagen über mögliche Kapazitätsengpässe des Systems, neuartige Zusammenhänge, die ein Fehlverhalten der Infrastruktur hervorbringen
- Implementierte Modelle im ITOA-System, die laufend im Betrieb die eintreffenden Daten analysieren und in Echtzeit Vorhersagen treffen



Phase 6 - Optimierung und Transformation

In der letzten Phase geht es darum, die gewonnenen Erkenntnisse für den IT-Betrieb zu nutzen. Anhand der Erkenntnisse können beispielsweise identifizierte Hardwareengpässe durch Zukauf neuer Hardware oder Fehlerbehebungsprozesse durch automatisierte Zuweisung von Tickets zu zuständigen Bearbeitern verbessert werden. Lernt ein ITOA-System beispielsweise, dass zu bestimmten Zeiten mehr Performance benötigt wird, können automatisch Cloud-Ressourcen zugeschaltet werden.

Zudem kann man einem Ausfall von Systemen vorbeugen. Fällt dem ITOA-System z.B. des Öfteren auf, dass die Temperatur im Rechenzentrum steigt und auch der physikalische Server stark ausgelastet ist, kann eine Erweiterung der Klimaanlage notwendig sein. Dies kann in diesem Schritt veranlasst werden. Ein weiteres Beispiel sind Speichermedien, die von den Servern mit Daten gefüllt werden bis kein freier Speicherplatz mehr vorhanden ist. Das System droht auch hier auszufallen. Das ITOA-System kann hier vorhersagen, wann eine Festplatte voraussichtlich voll sein wird und rechtzeitig eine neue bestellen, so dass es zu keinem Systemausfall kommt.

Im Ergebnis dieser Phase stehen:

- Handlungsempfehlungen auf Basis der Auswertungen
- Empfehlungen zur weiteren Implementierung des nächsten Reifegrades und zur Optimierung der ITOA-Architektur
- Schulung der Anwender zur Nutzung des ITOA-Systems, falls erforderlich

Zusammenfassung

Das vorliegende Whitepaper zeigt auf, dass mittels IT-Operations Analytics teure Ausfallzeit vermieden, die Zeiten zur Fehlerbehebung reduziert und die Gesamtpformance der IT gesteigert wird. Ein ITOA-System bietet einen Single-Point-of-Truth und ermöglicht somit eine Suche über alle IT-Betriebsdaten hinweg. Durch moderne Analysemethoden und Prognosemethoden, wie Machine-Learning, werden Ausfälle vorhergesagt und es kann ihnen so proaktiv entgegengewirkt werden.

Eine ITOA-Architektur besteht meistens aus einem Softwareagenten, der die Log-, Performance- oder Applikationsdaten sammelt, einem Logcollector bzw. einer Datenbank in dem diese Daten strukturiert gespeichert werden, sowie einem Logserver, der die Auswertung der verteilten Daten ermöglicht. Je nach Hersteller kommen hier jedoch unterschiedliche Datenbanken und Architekturen zum Einsatz.

ITOA-Hersteller bzw. Produkte gibt es derzeit ca. 90 am Markt. Als übergreifende ITOA-Tools haben sich HP Operations Analytics, IBM Operations Analytics und Splunk bewährt. Um zu identifizieren welches Tool die Bedürfnisse am besten erfüllt ist eine ausführliche Evaluierung zu empfehlen. Die wichtigsten Kriterien sollten hierbei die einfache Handhabung, Kosten, unterstützte Datenquellen, einfach Anpassbarkeit von Dashboards und Reports sowie die Qualität der Visualisierungen sein.

ITOA-Projekte bieten außerdem eine hohe Komplexität, daher sollten diese nach einem definierten Vorgehensmodell durchgeführt werden. In der Praxis haben sich die sechs Phasen „Definition der Strategie und Ziele“, „Ist-Analyse und Konzeption“, „Implementierung und Anbindung der Datenquellen“, „Datenanalyse“, „Modellierung und Auswertung“ sowie „Optimierung und Transformation“ bewährt. Das Vorgehen nach diesem Modell bietet einen strukturierten Leitfaden und führt dazu, dass auch ein komplexes Big-Data-Analytics-Projekt erfolgreich durchgeführt wird.



Kontaktieren Sie uns //

mayato GmbH
Am Borsigturm 9
13507 Berlin

info@mayato.com

+49 / 30 4174 4270 0