Die 8 größten Fehler

von IT-Experten und wie man sie vermeidet

splunk>
turn data into doing™

Inhalt

Der Status der globalen IT: Es muss kein aussichtsloser Kampf sein 2

#1 Zu viele Tools 4

#2 Spannungen zwischen IT und Business 6

#3 Kein einfacher Weg zum Ermitteln der Kernursache 8

#4 Falsche Qualifikationen für den Umgang mit Anwendungskomplexität 10

#5 Fehlende Transparenz bei der Cloud-Migration 12

#6 Überforderung durch Datensilos 14

#7 Keinen Plan für Systemausfälle 16

#8 Abhängigkeit von manuellen Prozessen 18

Was macht die IT wirklich… und was sollte sie eigentlich tun? 20

Transformation der IT: Erkennung, Untersuchung und Lösung beschleunigen – mit proaktivem Monitoring 22

Die Top-4-Werttreiber der IT Ops 24

Splunk-Lösungen 26

Fazit 28

Der Status der globalen IT: Es muss kein aussichtsloser Kampf sein

Stellen Sie sich vor, Sie seien Sisyphus, die bekannte Figur aus der griechischen Mythologie, die gezwungen ist, einen Felsbrocken einen Berg hinaufzuwälzen. Sobald der Felsbrocken oben ankommt, rollt er wieder herunter, sodass Sie das aussichtslose Unterfangen ein ums andere Mal wiederholen müssen. Für IT-Experten, die für eine komplexe, hybride Umgebung verantwortlich sind, dürfte das leider ein ziemlich vertrautes Szenario sein. Sie möchten Ihr Unternehmen voranbringen, doch stattdessen verbringen Sie die meiste Zeit damit, ein Problem nach dem anderen zu lokalisieren und zu beheben (also für immer und ewig Felsbrocken einen Berg hinaufzuwälzen). Als ob das noch nicht genug Stress wäre, stehen Sie auch noch unter dem Druck, die Systemverfügbarkeit und Performance aufrechtzuerhalten, um Kunden und Führungskräfte im Unternehmen bei Laune zu halten.

Mit diesem Problem stehen Sie nicht allein da. Weltweit sind IT-Experten für eine steigende Anzahl von Servern und Daten aus unterschiedlichen Datenquellen zuständig und verwenden viel zu viele Monitoring-Tools, um sinnvolle Erkenntnisse daraus zu gewinnen. Der Bericht *Reducing Complexity in IT Infrastructure Monitoring: A Study of Global Organizations*, der 2018 vom Ponemon Institute* veröffentlicht wurde, beleuchtet die Herausforderungen beim Troubleshooting und Monitoring von Cloud-basierten und lokalen Umgebungen. Das Ponemon Institute befragte 2.497 Experten für IT und IT-Sicherheit in Deutschland, den Vereinigten Staaten, dem Vereinigten Königreich, Frankreich, Australien, Singapur und Japan zu den Problemen, mit denen sie beim Monitoring ihrer Infrastruktur konfrontiert sind.

In Bezug auf das Vorjahr gab es folgende Aussagen:

- 24 Prozent erklärten, bei der Bewältigung der Größe und Komplexität der IT-Infrastruktur habe es Verbesserungen gegeben.
- 29 Prozent erklärten, die Bereitstellung und Wartung von Technologien zum Server-Monitoring sei einfacher geworden.

Außerdem war laut der Ponemon-Umfrage zwar ein beträchtlicher Prozentsatz der IT-Experten für die Überwachung von über 50 Servern zuständig, aber nur 33 Prozent der Befragten waren der Meinung, Performance und Systemverfügbarkeit mit ihren derzeitigen Tools sicherstellen zu können. Wie kann es der IT nun gelingen, immer komplexere, hybride Umgebungen effektiv zu verwalten, und welche wesentliche Missstände können IT-Organisationen beheben, um einen wirksameren Ansatz für Infrastruktur-Monitoring und Fehlerbehebung zu finden?

In diesem Leitfaden werden die **8 größten Fehler von IT-Experten** beleuchtet sowie Lösungen, Erkenntnisse und Beispiele aus der Praxis aufgezeigt, die Sie bei der Optimierung des IT-Monitorings und Troubleshootings in Ihrem Unternehmen unterstützen.

* Reducing Complexity in IT Infrastructure Monitoring: A Study of Global Organizations. Ponemon Institute, LLC. Erscheinungsdatum: April 2018

01

Zu viele Tools

70 Prozent der befragten IT-Experten erklärten, die Ermittlung der Kernursache auf der Grundlage von Daten sei zeitraubend. Die Erfassung und Normalisierung von Daten verschiedener Formate und Typen sei langwierig und kaum zu beherrschen, und es sei schwierig, Entscheidungen in Echtzeit zu treffen. Grund dafür ist häufig, dass Unternehmen zu viele Monitoring-Tools für einzelne Schichten ihres IT-Stacks, wie Netzwerke oder Anwendungen, verwenden. Dies führt zu Silos und Ineffizienz. Wenn Daten in einem Tool existieren, aber nicht auf Daten zugreifen oder mit Daten kommunizieren können, die ihrerseits auf andere Tools beschränkt sind, verlieren IT-Experten den Überblick über die Geschehnisse in ihrer Umgebung, weil ihnen die Zusammenhänge fehlen und sie nur einen Teil des Gesamtbilds sehen.

Die Lösung

Wie können Unternehmen nun das Monitoring ihrer IT-Infrastruktur verbessern? Laut IT-Experten sind bei der Auswahl einer Strategie für das Monitoring und die Fehlerbehebung in einer Infrastruktur folgende Faktoren entscheidend:

- Vereinfachung komplexer IT-Strukturen durch Konsolidierung von Technologien und Systemen
- Automatisierung von Prozessen für IT-Wartung und -Management

Es ist wichtiger denn je, die Performance in hybriden Architekturen mit einem Tool zu überwachen, das Daten aus allen Quellen sammelt und korreliert. Mehrere, fragmentierte Monitoring-Lösungen bieten nicht die Transparenz und Informationen, die zum Erreichen von Geschäfts- und IT-Zielen erforderlich sind. Welche Lösung gibt es also für das Problem zu vieler Tools und unterschiedlicher Daten? Die Antwort ist ein einzelnes, skalierbares Monitoring-Tool, das in hybriden Umgebungen operative End-to-End-Transparenz bietet. Sehen wir uns gemeinsam an, wie zwei Unternehmen das Problem gelöst haben.

ENGIE

VORHER: Die Lösung von Problemen wurde bei ENGIE immer zeitaufwendiger und ineffizienter, da die Entwicklungs- und Infrastruktur-Teams unterschiedliche Monitoring-Tools einsetzten und sich daher sehr häufig abstimmen mussten.

NACHHER: Durch den Einsatz von Splunk Enterprise und Splunk IT Service Intelligence (ITSI) gewann der große Energiekonzern einen kompletten Überblick über den Status wichtiger Geschäftsservices, konnte Probleme mit geschäftlichen Auswirkungen schneller beheben und die Zusammenarbeit zwischen den Entwicklungs- und Infrastruktur-Teams bei der Erstbeurteilung von Incidents optimieren.

SMSGlobal

VORHER: Der Online-Dienstleister SMSGlobal hatte Probleme mit dem Zugriff auf Informationen, da viele Anwendungen in unterschiedliche Geräte integriert waren – beispielsweise Cisco-Netzwerkgeräte und ASA-Appliances – und da jedes System Logs in unterschiedlichen Formaten und an verschiedenen Orten erzeugte.

NACHHER: Jetzt verwendet das Unternehmen Splunk Enterprise zum Sammeln, Indizieren und Auswerten von Betriebsdaten in der gesamten Infrastruktur und profitiert von detaillierter Echtzeittransparenz. Compliance-Berichte, an denen vorher zehn Mitarbeiter tagelang gearbeitet haben, lassen sich jetzt innerhalb von Sekunden von einem einzigen Administrator erstellen. Darüber hinaus erhielt das Unternehmen mit der Splunk App für Microsoft Exchange umfassende Einblicke in seine Microsoft Exchange-Umgebung. SMSGlobal kann nun E-Mail-Bewegungen in der gesamten IT-Infrastruktur in Echtzeit überwachen. Die für das Korrelieren von Events von Firewalls, Exchange oder Ad-Logs erforderliche Zeit konnte von mehreren Tagen auf Minuten reduziert werden.

02

Spannungen zwischen IT und Business

Da die Komplexität der digitalen Geschäftsinfrastruktur zunimmt, geraten IT-Teams beim Reduzieren geschäftskritischer Incidents stärker denn je unter Druck. Wenn IT-Systeme ausfallen, gehen die Auswirkungen über den unmittelbaren finanziellen Verlust durch Ausfallzeiten hinaus – Unternehmen können Kunden verlieren und ihren guten Ruf aufs Spiel setzen. Das ist die raue Wirklichkeit, die IT-Teams Tag und Nacht in Atem hält. In der Ponemon-Studie geben 61 Prozent der IT-Fachleute an, dass mangelnde Systemverfügbarkeit und eine schwache Performance zu Spannungen zwischen der IT und verschiedenen Geschäftsbereichen führen.

Die Lösung

Wie kann ein IT-Team Business-Experten und Entscheidungsträger dauerhaft zufriedenstellen? Ganz einfach: indem es sieben Tagen die Woche rund um die Uhr die Systemverfügbarkeit und eine starke -performance sicherstellt. Dies ist jedoch nur möglich, wenn die IT die Möglichkeit hat, Beeinträchtigungen schnell zu isolieren, zu erkennen und zu beheben, bevor sie zu einem Problem werden. Die IT braucht eine Lösung, mit der sich Kernursachen finden und Serviceunterbrechungen ermitteln lassen. Gleichzeitig müssen IT und Geschäftsbereiche zusammenarbeiten und geschäftliche sowie technische Anforderungen gemeinsam definieren.

Die nachfolgenden Praxisbeispiele zeigen, wie Unternehmen die Spannungen zwischen IT und Business reduzieren konnten.

Micron Technology, Inc.

VORHER: Das wachsende Fertigungsunternehmen Micron hatte aufgrund der fehlenden unternehmensweiten Transparenz über die gesamte IT-Infrastruktur hinweg mit Produktions- und Versandverzögerungen zu kämpfen.

NACHHER: Das Unternehmen führte einen analysegestützten Ansatz mit Splunk ein und transformierte damit seine IT Operations und das gesamte Business. Die Anzahl der geschäftskritischen IT Incidents konnte um mehr als 50 Prozent, die durchschnittliche Zeit bis zur Behebung von IT Incidents um 32 Prozent und die Anzahl größerer IT Incidents um 23 Prozent reduziert werden.

Networld Technology Ltd.

VORHER: Das IT-Team beim Online-Dienstleister Networld Technology stand aufgrund von zeitaufwendigen Datenaggregierungsverfahren unter Druck. Geschäftsentscheidungen wurden beispielsweise aufgrund von unzureichenden Such- und Monitoring-Funktionen für Analysen und einer fehlenden zentralen Sicht auf Vertriebsperformance und Umsätze verzögert. Das Businessteam musste die allgemeinen Trends verschiedener Handelsmarken zentral überwachen und für betriebswirtschaftliche Zwecke Top-Produkte, -Kategorien und -Händler ermitteln.

NACHHER: Mit Splunk Enterprise ersetzte Networld die manuelle Berichterstellung durch leistungsstarke Dashboards, die all diese Informationen in Echtzeit auf einer benutzerfreundlichen grafischen Oberfläche anzeigen, welche die Gesamtleistung der Website verfolgt. Die Abläufe wurden dank End-to-End-Transparenz von Geschäftsprozessen effizienter, und durch die Echtzeit-Umsatzanalyse wurden neue Geschäftschancen generiert.

03

Kein einfacher Weg zum Ermitteln der Kernursache

IT-Fachleute auf der ganzen Welt verbringen viel Zeit mit der Ermittlung und Behebung von Problemen in Serverumgebungen. Die beiden größten Herausforderungen für Fehlerbehebung, Monitoring und Cloud-Migration sind laut der Ponemon-Umfrage folgende:

- Fehlende Einblicke zum schnellen Lokalisieren von Problemen und Ermitteln der Kernursache
- Komplexität und Diversität von IT-Systemen und Technologie

Wenn Probleme von der IT nicht schnell erkannt und behoben werden können, hat dies unmittelbare geschäftliche Auswirkungen.

Die Lösung

Um Probleme schnell beheben zu können, benötigt die IT ein Monitoring-Tool, das die Kernursache eines Problems mit einer Warnmeldung zeigt, die darüber Auskunft gibt, wo und warum etwas schief läuft. Mithilfe einer Monitoring-Lösung, die Metriken und Protokolle korreliert und Visualisierungen von Warnmeldungen, Trends und Logs an einem einzigen Ort bereitstellt, kann die Zeit bis zur Problemlösung um die Hälfte reduziert werden.

Ganz entscheidend für den Erfolg ist, dass Ihr Monitoring-Tool diese Arten von Aktionen sowie eine Lösungsplanung ermöglicht. Nachfolgend erfahren Sie, wie zwei Unternehmen es geschafft haben, ihre Kernursachenanalysen zu beschleunigen.

AdvancedMD

VORHER: AdvancedMD, ein Cloud-basierter Anbieter für medizinische Fachkräfte, beklagte beim Auftreten von Problemen mangelnde Transparenz von servicebezogenen Systemen und damit einhergehende lange Erkennungs- und Behebungszeiten.

NACHHER: Das Unternehmen setzte Splunk ITSI ein und konnte mithilfe von Splunks konsolidierten Ansichten zu Workflows und Komponenten die Performance und Verfügbarkeit seiner Services sicherstellen, die MTTR (Mean-Time-To-Resolution) verkürzen und eine höhere Zuverlässigkeit erreichen.

Hyatt

VORHER: Der Online-Check-In der Hotelkette war aufgrund eines zeitaufwendigen Fehlerbehebungsprozesses nicht besonders zuverlässig.

NACHHER: Hyatt setzte zur Verkürzung der Erkennungszeit Splunk Enterprise und das Machine Learning Toolkit (MLTK) ein und profitiert damit von zentralen Echtzeiteinblicken. Dashboards und Warnmeldungen sorgen dafür, dass das IT-Team eine Beeinträchtigung bereits erkennt, bevor ein Ticket erstellt wird.

04

Falsche Qualifikationen für den Umgang mit Anwendungskomplexität

Als Ponemon IT-Fachleute nach den größten Risiken für erfolgreiche Fehlerbehebung, Migration in die Cloud und gelungenes Monitoring befragte, fielen die Antworten folgendermaßen aus:

- 55 Prozent nannten die zunehmende Komplexität der auf der Infrastruktur ausgeführten Anwendungen.
- 44 Prozent gaben einen Mangel an Qualifikation und Know-how im Umgang mit Anwendungskomplexität an.

Angesichts einer wachsenden und sich weiterentwickelnden Infrastruktur wird es für IT-Teams immer schwerer, die Systeme erfolgreich zu verwalten, zu überwachen und Fehler zu beheben. Darüber hinaus haben Unternehmen angesichts des Qualifikationsdefizits im IT-Bereich Schwierigkeiten, qualifizierte Fachkräfte anzuwerben und zu binden. Damit wird deutlich, warum IT-Teams unter Dauerdruck stehen.

Die Lösung

Wie können Unternehmen dafür sorgen, dass ihre IT-Teams beim Troubleshooting, Monitoring und der Migration in die Cloud effektiv arbeiten? Reibungslose IT Operations erfordern eine verlässliche Planung, in die zukünftiges Wachstum einfließt. Unternehmensführung und IT müssen gemeinsam an der Erstellung einer Roadmap für die IT-Umgebung arbeiten, gefolgt von einer auf diese Planung abgestimmten Fachkräftestrategie. Sie sollten folgende Punkte sicherstellen:

- Qualifikationsdefizite erkennen und mit Einstellungen entgegenwirken
- Qualifizierte Mitarbeiter ermitteln und entsprechend weiterentwickeln
- Nachfolgeplanung für unvermeidbare Änderungen sicherstellen

05

Fehlende Transparenz bei der Cloud-Migration

Welcher Aspekt bereitet bei der Cloud-Migration das meiste Kopfzerbrechen? 68 Prozent der IT-Experten gaben an, dass ihnen die Sicherstellung der Anwendungs-Performance und -Verfügbarkeit den größten Stress bereiten. Für über die Hälfte der Befragten waren die Kosten und die fehlende Möglichkeit, Anwendungen zu überwachen und Fehler zu beheben, die kritischsten Punkte.

Die IT muss auch bei einer immer komplexer werdenden Infrastruktur ihren Kernaufgaben wie Monitoring und Messen nachkommen. Wie kann es nun gelingen, eine transparente Infrastruktur zu schaffen und Einblicke in die Workloads zu geben, wenn Performance-Daten auf unterschiedliche Umgebungen verteilt sind?

Die Lösung

Ganz entscheidend ist es, die Performance in hybriden Architekturen mit einer Monitoring-Lösung zu überwachen, die Daten aus allen Speicherorten sammelt und korreliert. Während des gesamten Migrationsprozesses ist volle Transparenz erforderlich. Wählen Sie daher ein End-to-End-Monitoring-Tool, mit dem Sie Basiswerte vor der Migration, Zwischenergebnisse während der Migration und den Erfolg nach der Migration ermitteln können. Messen Sie vor der Cloud-Migration die Basiswerte für User Experience und Performance und definieren Sie akzeptable Niveaus nach erfolgter Migration. Um den Migrationserfolg genau überprüfen zu können, sollten Sie während des gesamten Migrationsprozesses dasselbe Monitoring-Tool verwenden. Ein einheitliches Tool analysiert zentralisierte Daten und bietet mithilfe von Dashboards und Berichten aussagekräftige Informationen.

REI

VORHER: REI wollte bei der Migration von Anwendungen zu Amazon Web Services (AWS) sein Sicherheitsniveau durch die Einbindung von Edge-Schutz für seine Amazon Virtual Private Clouds (VPCs) erhöhen. Dabei wurde dem Unternehmen klar, dass Echtzeittransparenz bei Anwendungen, Services und der Sicherheitsinfrastruktur erforderlich war, um während der Cloud-Migration umfassenden Schutz zu gewährleisten und eine Sicherheitslücke zu schließen.

NACHHER: REI setzte in seiner hybriden Umgebung Splunk Cloud und Amazon GuardDuty ein und konnte dadurch unter anderem von End-to-End-Sicherheitstransparenz während der AWS-Cloud-Migration sowie von Echtzeiterkenntnissen über potenzielle Bedrohungen profitieren.

TrueCar

VORHER: TrueCar, ein digitaler Automobilmarktplatz, setzte ein Open-Source-Tool für das Log-Management ein, dessen Wartung viel Zeit in Anspruch nahm.

NACHHER: Als das Unternehmen auf Splunk Cloud umstieg, gewann das Infrastruktur-Team Zeit für die Lösung anderer Probleme. Das Team setzt nun Splunk Cloud unternehmensweit für das Monitoring der gesamten Kerninfrastruktur und Anwendungsbereitstellung ein. Dashboards bieten Transparenz für die AWS-Abrechnung und versetzen das Team in die Lage, die Kosten besser zu kontrollieren und die Ressourcen während der Cloud-Migration von TrueCar effektiv zuzuweisen, ohne die Infrastruktur verwalten zu müssen.

Mit Blick auf die Migrationsausgaben zeigen Kostenmanagement-Tools Daten zur aktuellen und historischen Nutzung von Instances sowie ungenutzte Ressourcen. Um belastbare Prognosen zu den Ressourcen erstellen und intelligente Migrationsentscheidungen treffen zu können, sind umfassende Einblicke in die Wirtschaftlichkeit der gesamten Infrastruktur entscheidend. Weitere Informationen zum Erstellen einer effektiven Migrationsstrategie mit Kostenprognose und -management finden Sie im Leitfaden „Die richtige Strategie für Ihre Cloud-Migration“.

06

Überforderung durch Datensilos

Wenn sich die Infrastruktur hin zu einer Mischung aus Mainframe-, Client-Server-, virtualisierter, serverloser und hybrider Cloud entwickelt, erhöht sich damit auch die Wahrscheinlichkeit von Silos und blinden Flecken. Als Ponemon IT-Fachleute nach den größten Schwierigkeiten beim Verwalten der IT-Infrastruktur befragte, standen Komplexität und Diversität von IT-Systemen ganz oben auf der Liste.

Die Komplexität der Infrastruktur beeinträchtigt die Fähigkeit der IT-Abteilung, die Kernursache eines Problems schnell zu ermitteln. Auf die Frage nach den Herausforderungen, mit denen sie beim Ermitteln der Kernursache konfrontiert sind, gaben 63 Prozent der IT-Experten an, es sei problematisch, Daten aus verschiedenen Formaten zu erfassen und sinnvolle Erkenntnisse daraus zu gewinnen, um Diagnosen zu erstellen und die Kernursache zu bestimmen. 56 Prozent erklärten sogar, sie seien noch nicht einmal sicher, welche Daten für bestimmte Probleme relevant seien.

Die Lösung

Zur Vermeidung von Silos und blinden Flecken braucht die IT eine Einzellösung für Infrastruktur-Monitoring und Troubleshooting, die in der Lage ist, Daten aus beliebigen Quellen zu erfassen und zu korrelieren. Wenn separate Monitoring- und Log-Analyse-Tools durch eine einzelne Lösung ersetzt werden, die Metriken und Logs korreliert, lässt sich die Ermittlung der Kernursache beschleunigen. Sehen wir uns an, wie zwei Unternehmen ihre Probleme mit Datensilos gelöst haben.

Leidos

VORHER: Das IT-Team von Leidos, einem führenden Anbieter von Lösungen für Wissenschaft und Technologie, hatte Probleme, Störungen zu finden und zu beheben, bevor diese sich negativ auf die Kundenerfahrung auswirken. Die Ursache lag darin, dass die Mitarbeiter Muster und Trends in isolierten Datensilos finden und eine Flut von Events aus mehr als 120 IT-Services sichten mussten.

NACHHER: Nach der Einführung von Splunk war das Unternehmen in der Lage, Daten über den gesamten Service-Stack hinweg zu sehen, Events aus der heterogenen IT-Umgebung zu konsolidieren, doppelte Warnmeldungen zu erkennen und zu unterdrücken, gelöste Warnmeldungen zu löschen und auf Events mit Handlungsbedarf runterzubrechen. Splunk hilft dem Unternehmen, 3.500 bis 5.000 tägliche Warnmeldungen auf rund 50 Tickets zu reduzieren, auf die der Netzwerk- und Rechenzentrumsbetrieb reagieren kann.

Micron

VORHER: Micron hatte Schwierigkeiten mit der Aufrechterhaltung der für die Wettbewerbsfähigkeit erforderlichen Servicequalität, da man aufgrund von Datensilos nur begrenzt in der Lage war, IT-Probleme zu identifizieren, zu lösen und zu verhindern.

NACHHER: Das Technologieunternehmen führte einen analysegestützten Ansatz mit Splunk ein und transformierte damit seine IT Operations und das gesamte Business, wodurch die Lösungszeit erheblich verkürzt und die Anzahl der IT Incidents gesenkt werden konnte. Dank Echtzeittransparenz können Engineering-Teams nun Daten und Fachwissen teilen, und eine neue IT Operations-Strategie ermöglicht ein frühzeitiges Erkennen von Problemen zur Vermeidung negativer geschäftlicher Auswirkungen.

07

Keinen Plan für Systemausfälle

Die meisten Unternehmen sind nicht auf Serviceunterbrechungen oder -ausfälle vorbereitet. Im Rahmen der Ponemon-Studie gaben nur 29 Prozent der IT-Experten an, ihr Unternehmen verfüge über:

- Dokumentierte Workflows und automatisierte Prozesse für den Fall eines Systemausfalls
- Die Fähigkeit, Probleme dank Automatisierung und aktueller Monitoring-Toolsets frühzeitig zu lokalisieren

Je länger die Behebung eines Incidents dauert, desto länger leiden Kunden unter einer schlechten Kundenerfahrung und Unternehmen unter negativen geschäftlichen Auswirkungen wie Umsatzeinbußen. Ohne dokumentierte, ausführbereite Pläne für das Incident Management, wird in Unternehmen viel kostbare Lösungszeit für potenziell wiederkehrende Probleme statt zum Reflektieren und Lernen aufgewendet.

Die Lösung

Unternehmen sollten sich auf das Schlimmste vorbereiten, indem sie einen Notfallplan für einen Ausfall des IT-Systems einrichten. Inhaberschaft und Zuständigkeiten sollten klar definiert sein, und die IT sollte einen Plan für jedes potenzielle Technologieausfall-Szenario dokumentieren. Ganz entscheidend ist es dabei, einen Systemnotfallplan immer wieder zu testen, damit er auch wirklich funktioniert. Beachten Sie außerdem, dass jeder Notfallplan im Fall von Infrastrukturänderungen weiterentwickelt werden muss. Es kommt darauf an, zur richtigen Zeit die richtigen Informationen den richtigen Personen – oder Teams – zukommen zu lassen.

08

Abhängigkeit von manuellen Prozessen

Weltweit wenden IT-Teams zu viel Zeit für manuelle Aufgaben auf, beispielsweise bei der Durchführung von Suchen, dem täglichen Log-Management, der Fehlerbehebung oder der Erstellung von Analysen und Compliance-Berichten. Da den IT-Teams der Überblick über die gesamte Infrastruktur fehlt, können sie nur reaktiv handeln und müssen zeitintensive manuelle Prozesse ausführen. Nur 30 Prozent der IT-Experten geben an, dass ihr Unternehmen proaktiv Daten aus unterschiedlichen Informationsquellen zusammenträgt, um Beeinträchtigungen zu erkennen, bevor es zu einem Ausfall kommt.

In Kombination mit Problemen bei der Ressourcenzuweisung führt die Abhängigkeit von manuellen Prozessen zu einer längeren MTTR (Mean-Time-To-Resolution), was wiederum negative Auswirkungen auf die Kundenerfahrung und Spannungen zwischen der IT- und Business-Seite nach sich ziehen kann.

Die Lösung

Wie kann die IT nun den Wechsel von reaktivem zu proaktivem Handeln schaffen? Komplexe Vorgänge beim Infrastruktur-Monitoring können mit Monitoring-Tools vereinfacht werden, die auf Monitoring und Fehlerbehebung in der Cloud oder einer lokalen Umgebung ausgelegt sind. Es ist keine große Überraschung, dass sich 87 Prozent der IT-Experten auf die Frage, welche Funktion sie sich von einer Monitoring-Lösung am dringendsten wünschen, für automatisierte, auf Machine Learning basierende Untersuchungen aussprachen, die ihnen ein rasches und problemloses Erkennen von Trends und Kernursachen ermöglichen. Weitere wichtige Merkmale einer Monitoring-Lösung sind eine einfache Installation und Bereitstellung und dass sie über verschiedenste Teams, Anwendungsfälle sowie hybride Umgebungen hinweg eingesetzt werden kann.

Durch die Implementierung von Automatisierung und Operations Analytics wendet die IT weniger Zeit für die Behebung von Problemen auf und kann sich stattdessen verstärkt auf Verbesserungen konzentrieren. Darüber hinaus steigt damit laut 51 Prozent der IT-Experten die Chance, Projekte im Rahmen des Budgets abzuwickeln. 46 Prozent gaben an, dadurch würde sich die Fähigkeit verbessern, Projekte fristgerecht abzuschließen, und 45 Prozent erklärten, damit lasse sich die Servicequalität besser aufrechterhalten.

Mit dem richtigen Tool ist der Übergang von reaktivem Monitoring zu proaktivem Echtzeit-Monitoring machbar. Diese Erfahrung haben auch die nachfolgenden Unternehmen gemacht.

SONIFI

VORHER: SONIFI, ein Technologie-Integrator für Unternehmen in Gastgewerbe und Gesundheitssektor, brauchte eine Lösung für langwierige, manuelle Prozesse, die fundierte, datengestützte Entscheidungen erschwerten.

NACHHER: Seit SONIFI Splunk Enterprise einsetzt und von neuen Funktionen wie Metriken und Event-Annotation profitiert, konnte das Unternehmen durch eine Zentralisierung der Berichterstellung und die Implementierung optimierter Prozesse jährliche Einsparungen in Höhe von 85.000 USD erzielen. Hinzu kamen dank neuer Einblicke in Abrechnungsentscheidungen monatliche Einsparungen in Höhe von 100.000 USD sowie eine Verkürzung der Zeit zur Berichterstellung von Tagen auf Minuten.

ROKT

VORHER: Das IT-Team des Online-Dienstleisters ROKT verbrachte Stunden mit der manuellen Verwaltung seiner verschiedensten Logs, die unter anderem Benutzer-, Zugriffs-, Lastenausgleichs-, CloudTrail-, System-, Kunden- und Transaktionsprotokolle umfassten.

NACHHER: Splunk optimierte das Log-Management des Unternehmens. Das zentralisierte Log-Analyse-Tool für maschinengenerierte, unstrukturierte und strukturierte Daten versetzt IT-Manager in die Lage, alle Logs in virtuellen und nicht-virtuellen Umgebungen von einer zentralen Stelle aus automatisch zu indizieren, zu korrelieren und zu überwachen. Mit wenigen Mausklicks verwandeln sich manuelle Suchen in automatisierte Echtzeit-Warnmeldungen, grafische Berichte und intuitive Dashboards. Vorgänge, für deren Abwicklung das Team zuvor Stunden gebraucht hatte, ist nun innerhalb von Minuten automatisch erledigt, sodass das Unternehmen weiter florieren und wachsen kann.

Was macht die IT wirklich… und was sollte sie eigentlich tun?

Angesichts der Vielzahl von Servern, Anwendungen und Events, die es zu überwachen gilt, haben IT-Fachleute alle Hände voll damit zu tun, Erwartungen an Performance und Verfügbarkeit zu erfüllen. Außerdem sollen sie den Geschäfts-anforderungen gerecht werden, sämtliche Dinge schneller entwickeln und bereitstellen und in der gesamten Struktur für höhere Qualität und Effizienz sorgen. Und dann erwartet man von ihnen auch noch, dass sie dies alles mit weniger Ressourcen bewältigen, denn laut der Ponemon-Umfrage sollen die Budgets für lokale und Cloud-IT in den meisten Fällen im nächsten Jahr nicht erhöht werden.

In Anbetracht der Tatsache, dass die IT für die Verwaltung großer Portfolios immer komplexerer (stacked) Technologien zuständig ist, auf Geschäftsanforderungen reagieren, Serviceanfragen erfüllen und Probleme in der Produktion lösen muss, wenn etwas schiefgeht, wird eines klar: Es ist schwierig für IT-Teams, die Unternehmensanforderungen zu erfüllen, ohne von einem rein reaktiven Monitoring auf ein proaktives – oder gar prädiktives – Monitoring umzusteigen.

Worauf sollte sich die IT wirklich konzentrieren?

- Ausfälle vermeiden
- Kundenerfahrung verbessern
- Agil sein und sich an stetig wechselnde Geschäftsanforderungen anpassen

Wie kann die IT nun weniger reaktiv und dafür stärker proaktiv werden? Der Wechsel von reaktivem Monitoring und Troubleshooting zu einem proaktiven Ansatz wird mit einer analysegestützten Monitoring-Lösung wie Splunk möglich, die intelligente Untersuchungen und eine beschleunigte Kernursachenanalyse erlaubt.

Transformation der IT:
Erkennung, Untersuchung und Lösung beschleunigen – mit proaktivem Monitoring

Bei Splunk hören wir von einem Kunden nach dem anderen, dass stetig wechselnde Anforderungen einen neuen Ansatz beim Infrastruktur-Monitoring erforderlich machen. In allen Branchen, in denen wir tätig sind – von Finanzdienstleistungen über das Gesundheitswesen, die verarbeitende Industrie und Telekommunikation bis hin zum Technologiesektor –, haben IT-Teams mit mangelnder Transparenz ihrer Gesamtinfrastruktur, langwierigen Untersuchungen und einer langen MTTR (Mean-Time-To-Resolution) zu kämpfen.

Das sagen Kunden über Herausforderungen beim Infrastruktur-Monitoring		
Monitoring und Problembehebung in Silos	Zunehmende Komplexität erschwert das Ermitteln und Beheben von Problemen	Zu viel Zeitaufwand für die Verwaltung der Monitoring-Software
„Warum läuft das Monitoring über ein Tool und die Fehlerbehebung über ein anderes?“	„Die Anwendungen werden immer komplexer und ich soll mehr überwachen als je zuvor und auch noch Probleme schneller lokalisieren!“	„Wir haben nicht genügend Ressourcen für den Erwerb und die Wartung komplexer Monitoring-Tools.“

Welchen Beitrag kann Splunk zur Lösung der Probleme beim Infrastruktur-Monitoring leisten?

Unsere Kunden konnten mit Splunk erhebliche Verbesserungen bei Monitoring und Troubleshooting erzielen, unter anderem:

- Optimierte Erkennungszeiten
- Schnellere Sichtung und Untersuchung
- Raschere Wiederherstellung von Services
- Beschleunigte Kernursachenanalyse, sodass Trends beim Incident Response dokumentiert und Planungen entsprechend durchgeführt werden können.

Splunk-Kunden berichten außerdem von Kosteneinsparungen im Zusammenhang mit der Kapazitätsauslastung der Infrastruktur sowie von der Möglichkeit, über die bloße Fehlerbehebung hinauszugehen und Effizienzlücken zu finden.

Die **Top-4-Werttreiber** der IT Ops

VOR SPLUNK

Ausfaller-kennung	**Incident-Sichtung**	**Incident-Troubleshooting**	**Service-Wiederherstellung**	**Kernursachen-analyse**
Oft informiert ein Kunde die IT	Alle verfügbaren Kräfte, 30 bis 40 Minuten	Langwierige manuelle Log-Analyse	Fix wird implementiert	Bis zu 30 % unbekannte Kernursachen führen zum erneuten Auftreten von Incidents

MIT SPLUNK

#1 Bessere Erkennung: Kunde wird von IT benachrichtigt

#3 Schnellere Untersuchung (MTTI) durch schnelle Log-Suche und Korrelation, die von unterschiedlichen Teams gemeinsam ausgeführt wird (alle sehen dieselben Daten)

Fix wird implementiert

#2 Raschere Sichtung, oft durch 1st-Level-Mitarbeiter ohne Einsatz aller verfügbaren Kräfte

#4 Schnellere und umfassendere Kernursachenanalyse reduziert erneutes Auftreten von Incidents

Kunden-Feedback:

- **15-45 %** weniger Incidents mit hoher Priorität
- **70-90 %** weniger Zeitaufwand für die Untersuchung von Incidents
- **67-82 %** weniger Incident-Auswirkungen auf das Unternehmen
- **5-20 %** mehr Kapazitätsauslastung der Infrastruktur

Splunk-Lösungen

Splunk bietet „Insights“-Produkte für neue Splunk-User, die jeweils auf einen bestimmten Anwendungsfall ausgelegt sind. **Splunk Insights for Infrastructure (SII)** ist ein leistungsstarkes, benutzerfreundliches Server-Monitoring-Tool ohne Begrenzung bei der Anzahl von Benutzern, Hosts und Warnmeldungen. SII vereint nahtlos Metriken (für das Monitoring) und Logs (für die Problembehebung) aus AWS-, Linux- und Windows-Umgebungen in einer einzelnen Benutzeroberfläche. Korrelieren Sie Metriken und Logs in vielen unterschiedlichen, sofort einsetzbaren Dashboards und Visualisierungen, nehmen Sie Gruppierungen nach Entitäten vor und dringen Sie schneller zur Kernursache vor. Download und Installation sind denkbar einfach, und mithilfe von vordefinierten, blitzschnellen Dashboards gewinnen Sie innerhalb weniger Minuten neue Erkenntnisse. Kein Hin- und Herschwenken zwischen unterschiedlichen Monitoring-Tools mehr. SII ist für den Einstieg kostenlos verfügbar und wird für größere Speicheranforderungen zu wettbewerbsfähigen Preisen in Form von Jahresverträgen angeboten.

Für bestehende Splunk Enterprise-Kunden bietet die **Splunk App for Infrastructure** dieselbe Erfahrung wie Splunk Insights for Infrastructure, verfügt jedoch darüber hinaus über Plattformfunktionen, z. B.:

- Native, effiziente und skalierbare Indizierung von Metriken
- Splunks leistungsfähige SPL-Abfragesprache (Search & Reporting App)
- Rollenbasierte Zugriffssteuerung
- Möglichkeit, Server-Metriken und Logs mit Daten aus allen Schichten des IT-Stacks zu korrelieren

> „Splunk Insights for Infrastructure bietet eine intelligente Kombination aus Metriken und Protokollierung für eine umfassendere Sicht auf die Infrastruktur-Performance. Wir können damit ungewöhnliches Verhalten wie beispielsweise einen CPU-Spike erkennen und es mit Protokollen korrelieren, um Probleme viel schneller zu beheben.“
>
> **— Daryl Robbins,** Sr. Cloud Architect, Entrust Datacard

Fazit

Angesichts von Problemen wie mangelnder Transparenz bei der Cloud-Migration und der Abhängigkeit von manuellen Prozessen stehen Unternehmen beim Troubleshooting und Monitoring hybrider Umgebungen vor einem harten Stück Arbeit. Es liegt auf der Hand, dass die IT eine Lösung zum effektiven Umgang mit immer komplexeren Umgebungen benötigt – eine Lösung, die den Wandel von einer reaktiven zu einer proaktiven und schließlich zu einer prädiktiven IT ermöglicht.

Splunk kann Sie durch folgende Funktionen bei der Lösung vieler Herausforderungen, mit denen Sie derzeit konfrontiert sind, unterstützen:

- Korrelierte Metriken und Logs für besseres Monitoring und schnellere Problembehebung
- Nahtloses, metrik- und protokollbasiertes Monitoring und Troubleshooting
- Automatisierte Untersuchungen zum einfachen Ermitteln von Trends und Kernursachen

Der Einstieg in Splunk ist denkbar einfach:

Splunk Insights for Infrastructure steht kostenlos zum Download zur Verfügung und beinhaltet eine Storage-Lizenz über 200 GB, die für das Monitoring von etwa 50 Servern (abhängig von Ihrer Umgebung und dem Monitoring-Umfang je Server) ausreicht. Ebenso ist Community-Support mit eingeschlossen. Die Download-Version ist zeitlich nicht beschränkt, Sie können die Software also dauerhaft kostenlos nutzen! Sie können zusätzliche Speicherkapazität mit Basissupport von splunk.com oder Ihrem bevorzugten Splunk-Vertriebspartner erwerben. Starten Sie noch heute unter splunk.com/insights-for-infrastructure.

Splunk App for Infrastructure ist für bestehende Splunk-Kunden gedacht, die bereits über eine Enterprise-Bereitstellung und -Lizenz verfügen. Die App ist auf Splunkbase zum Download verfügbar.

* Reducing Complexity in IT Infrastructure Monitoring: A Study of Global Organizations. Ponemon Institute, LLC. Erscheinungsdatum: April 2018

Legen Sie los.

Tauchen Sie tiefer in das ein, was Ihre Systeme, Services und Apps wirklich tun. Lesen Sie „Observability: Ein Leitfaden für Einsteiger“.

20-SPLK-8-Biggest-Mistakes-IT-Practitioners-Make-109-EB

splunk> turn data into doing™