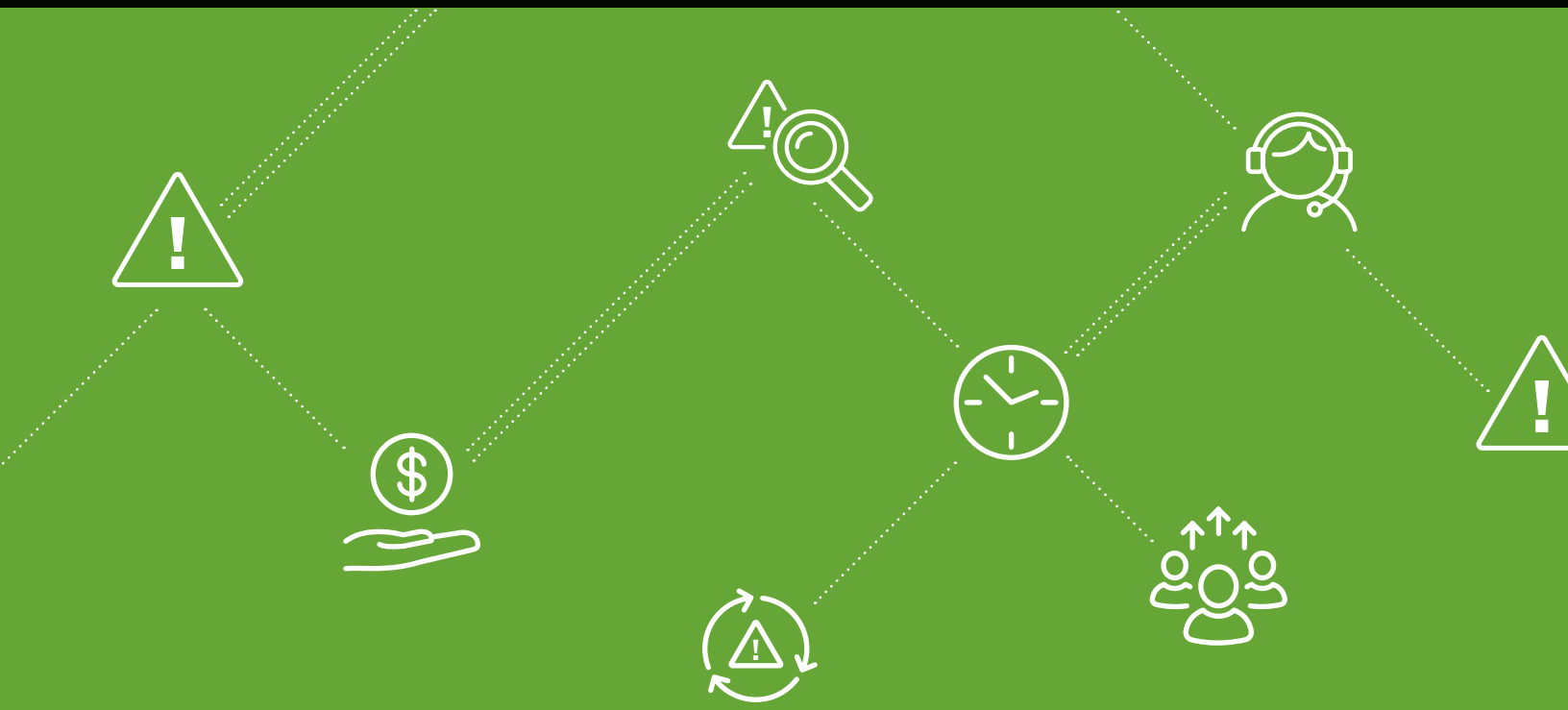
splunk> | quocirca

FORSCHUNGSANALYSE

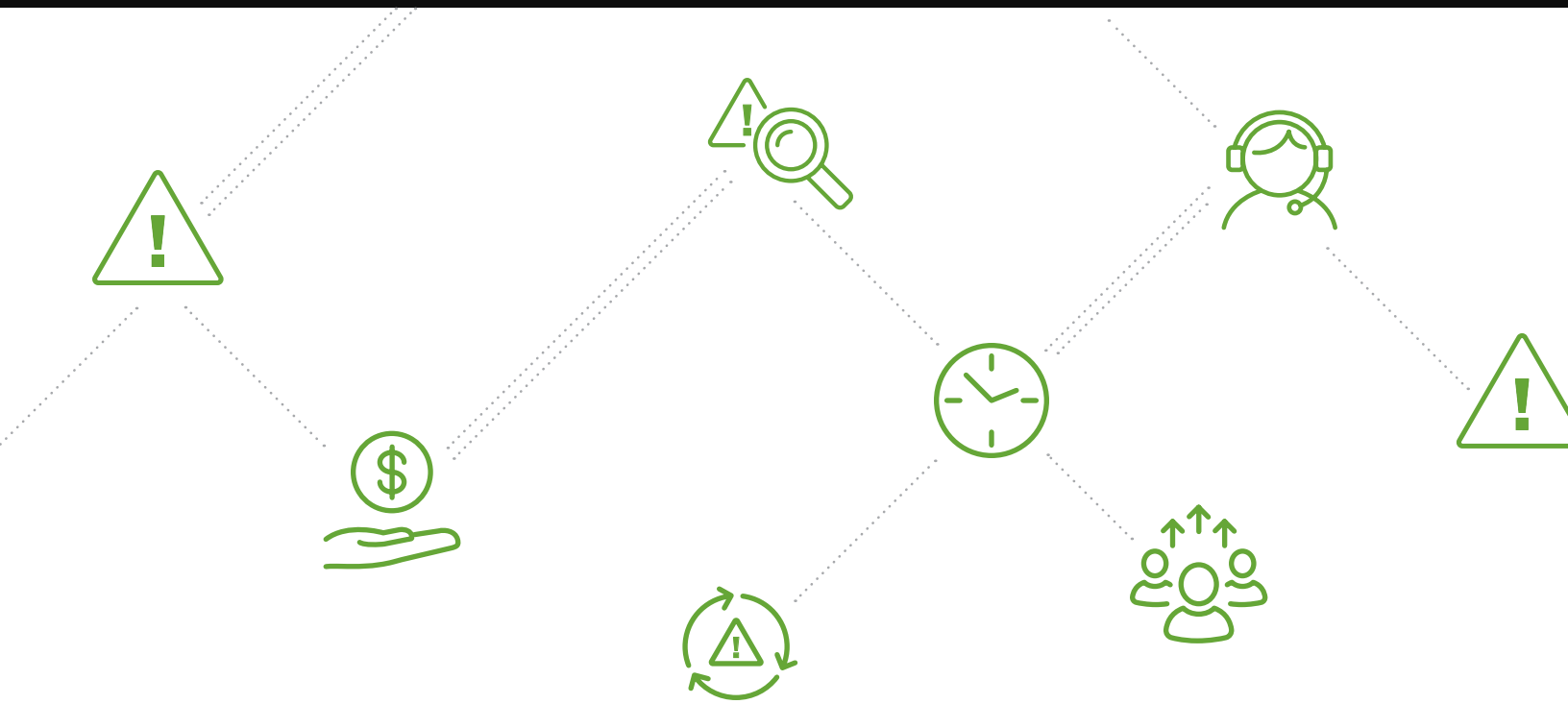


SCHADENSBEGRENZUNG

Die Auswirkungen kritischer IT Incidents

Von Bob Tarzey, Analyst und Director, Quocirca

November 2017



SCHADENSBEGRENZUNG

Die Auswirkungen kritischer IT Incidents

Von Bob Tarzey, Analyst und Director, Quocirca
November 2017

IT Incidents verursachen jährliche Kosten in Millionenhöhe für Unternehmen aller Branchen. Die Behandlung von Incidents hält IT-Mitarbeiter von anderen Aktivitäten ab, und über die IT-Abteilung hinaus wirken sich Incidents auf die Geschäftsproduktivität und die Kundenerfahrung aus.

Ein durchschnittliches Unternehmen hat jede Woche mit Hunderten von Incidents zu tun. Die IT-Systeme und Infrastrukturen, die diesen Incidents zugrunde liegen, erzeugen riesige Datenmengen. Das Sammeln und Analysieren dieser Daten aus den verschiedenen beteiligten IT-Systemen führt zu einer schnelleren und effizienteren Erkennung von Incidents, einer besseren Problembehebung und einer kürzeren MTTR (Mean Time to Repair). Event-Daten können auch zur Kernursachenanalyse beitragen und helfen, das erneute Auftreten eines Problems zu vermeiden. Durch die Zeitersparnis bei der Behandlung von IT Incidents bleibt den IT-Mitarbeitern mehr Zeit, sich auf digitale Innovationen zu konzentrieren, anstatt ständig dafür zu kämpfen, den Betrieb aufrecht zu erhalten.

KURZFASSUNG

Incidents und kritische Incidents

Ein durchschnittliches Unternehmen protokolliert etwa 1.200 IT Incidents pro Monat, von denen fünf kritisch sind. Es ist eine echte Herausforderung, alle Daten von den an diesen Incidents beteiligten Events zu durchforsten, um sie anschließend für die Event-Behandlung zu priorisieren. 70% der Befragten geben an, dass ein früherer kritischer Incident den Ruf ihres Unternehmen geschädigt hat, was die Bedeutung einer frühzeitigen Incidents-Erkennung und Schadensbegrenzung unterstreicht.

Die Kosten kritischer Incidents für IT und Unternehmen

Die durchschnittlichen IT-Kosten eines kritischen Incidents belaufen sich auf 36.326 USD. Die nachgelagerten Kosten für das Unternehmen betragen im Durchschnitt weitere 105.302 USD. Diese beiden Kosten steigen zusammen an, was darauf hindeutet, dass hohe IT-Kosten ein Indikator für schlechtes Event und Incident Management sind, was sich wiederum auf den Geschäftsbetrieb auswirkt.

Durchschnittsdauer für die Erkennung, für die Behebung und die Durchführung von Kernursachenanalysen

80% der Studienteilnehmer geben an, dass sie ihre Durchschnittdauer zur Erkennung von Incidents verbessern könnten, was zu einer kürzeren MTTR führen und die Auswirkungen auf das Unternehmen verringern würde. Die MTTR für kritische Incidents beträgt 5,81 Stunden. Dieser Wert verringert sich, wenn von vorneherein weniger Incidents zu behandeln sind. Im Durchschnitt werden weitere 7,23 Stunden für die Kernursachenanalyse aufgewendet, welche in 65% der Fälle erfolgreich ist.

Unnötige Incidents

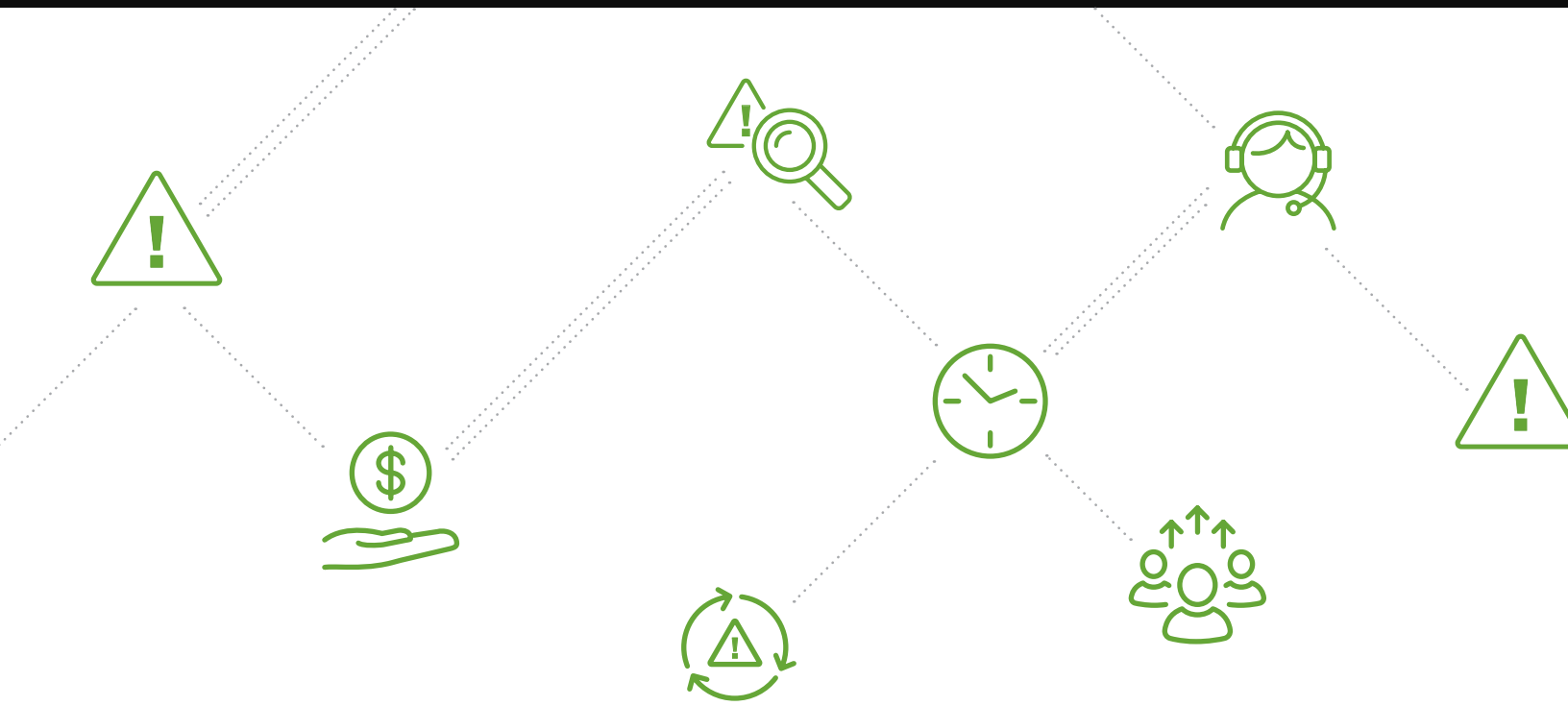
Doppelte und wiederholt auftretende Incidents sind ein weit verbreitetes Problem. 97% sagen, dass ihr Event Management-Prozess zu Dubletten führt, sodass mehrere Incidents für dasselbe IT-Problem erzeugt werden; 17,2% aller Incidents sind Dubletten. 96% geben an, dass es zu Wiederholungs-Incidents führt, wenn man nicht durch eine effektive Kernursachenanalyse aus früheren Incidents lernt; 13,3% aller Incidents sind Wiederholungs-Incidents.

Transparenz der IT-Infrastruktur

Das Monitoring der IT-Infrastruktur zur Protokollierung und Identifizierung von Incidents könnte verbessert werden. 80% geben an, dass es bei ihnen "blinde Flecken" gibt, die zu einer verzögerten Erkennung und Untersuchung von Incidents führen. Aufgrund der Komplexität von IT-Systemen und zugehörigen Monitoring-Tools fehlt vielen Unternehmen eine angemessene, holistische End-to-End-Sicht auf ihre IT-Infrastruktur.

Bewältigung des Event-Volumens und Event Management

Die Bewältigung der von IT-Monitoring-Tools erzeugten Event-Mengen ist eine echte Herausforderung. 52 % der Befragten geben an, dass sie gerade so zurechtkommen, 13 % haben Schwierigkeiten mit der Event-Flut und 1 % sind überfordert damit. Unternehmen mit Event-Managementprozessen, die ein einfaches Management des Event-Volumens ermöglichen, weisen eine kürzere mittlere Incident-Erkennungszeit sowie weniger Incident-Dubletten und Wiederholungs-Incidents auf.



EINLEITUNG

Dieser Bericht stellt neue Untersuchungsergebnisse dazu vor, welche Auswirkungen die Menge von IT-Incidents auf Unternehmen hat. Insbesondere wurden dabei kritische Incidents untersucht, die Geschäftsprozesse stoppen und sich auf Anwender und Kunden auswirken können. Untersucht werden die bestehenden Möglichkeiten zur Verarbeitung der enormen Menge an Event-Daten, die von den IT-Monitoring-Tools erzeugt werden, die Möglichkeiten zur Vermeidung von Incident-Dubletten sowie zur Reduzierung der durchschnittlichen Erkennungszeit (Mean Time to Detect, MTTD) und der MTTR (Mean Time to Repair). Außerdem widmet sich der Bericht der Fragestellung, wie durch Kernursachenanalyse künftige Incident-Wiederholungen vermieden werden können. Die frühzeitige Erkennung von Incidents reduziert die Auswirkungen der nachgelagerten Faktoren und die Kosten von Incidents sowohl für IT-Abteilungen als auch für die zugehörigen Unternehmen.

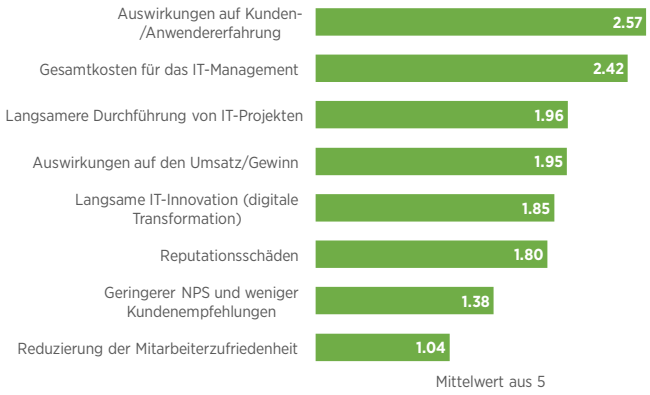
Die Untersuchung wurde in neun Ländern durchgeführt: USA, Japan, Singapur, Australien, Schweden, Niederlande, Deutschland, Frankreich und Großbritannien. Sie umfasste verschiedene Unternehmensgrößen und Branchen (siehe Anhang).

IT INCIDENTS UND KRITISCHE INCIDENTS

Mit der zunehmenden IT-Abhängigkeit von Unternehmen wird ihre IT-Infrastruktur immer komplexer. Der Druck, neue digitale Initiativen zu unterstützen und wettbewerbsfähig zu bleiben, führt zu neuen Schichten der IT-Infrastruktur, einschließlich Virtualisierung, Containerisierung und Cloud-Services. Dies führt zu frustrierten Anwendern und ungewollten Geschäftskosten und kann Reputationsschäden nach sich ziehen.

Die Untersuchungen zeigen, dass Incidents am kritischsten sind, wenn sie Auswirkungen auf die Anwendererfahrung haben oder die Projektdurchführung verlangsamen (Abbildung 1). Für IT-Management-Teams müssen alle Event-Daten, die von den Monitoring-Tools der IT-Infrastruktur generiert werden, gefiltert werden, um die relevanten Events festzustellen, sodass Probleme behoben und eine rechtzeitige Wartung durchgeführt werden können. IT-Teams brauchen Unterstützung, um die Event-Flut zu sichten und die Probleme zu erkennen, die behandelt werden müssen. Wenn kleine Probleme nicht rechtzeitig erkannt und behoben werden, können sie unnötigerweise zu kritischen Incidents werden.

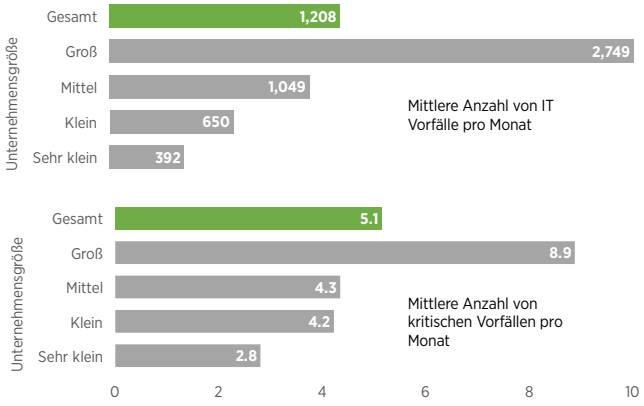
Figure 1: Mögliche Konsequenzen eines IT Incidents, die am meisten beunruhigen



Unternehmen verzeichnen 5,1 kritische Incidents pro Monat

Die höchste Priorität muss kritischen Incidents eingeräumt werden (von Service Desk-Systemen als Schweregrad 1, Priorität 1 oder P1 bezeichnet). Ein durchschnittliches Unternehmen protokolliert etwa 1.200 IT Incidents pro Monat, von denen 5,1 kritisch sind (Abbildung 2). 70% der Befragten geben an, dass ein früherer kritischer Incident den Ruf ihres Unternehmen geschädigt hat. Es kann für IT-Teams schwierig sein, zu wissen, was kritisch ist und was nicht; sie brauchen Unterstützung, um Events möglichst effizient zu sichten und zu priorisieren.

Figure 2: Durchschnittliche Anzahl an IT Incidents und kritische Incidents, die pro Monat anfallen



70% geben an, dass ein kritischer Incident den Ruf ihres Unternehmen geschädigt hat

DIE KOSTEN KRITISCHER INCIDENTS

Die durchschnittlichen IT-Kosten eines kritischen Incident belaufen sich auf 36.326 USD. Dazu kommen durchschnittliche Kosten für das Unternehmen in Höhe von 105.302 USD (Abbildung 3). Diese beiden Kosten steigen zusammen an, was darauf hindeutet, dass hohe IT-Kosten ein Indikator für schlechtes Incident Management sind, was sich wiederum auf den Geschäftsbetrieb auswirkt.

IT-Durchschnittskosten eines kritischen Incident betragen 36.326 USD

Durchschnittskosten eines kritischen Incident für das Unternehmen betragen 105.302 USD

Die Gesamtkosten eines kritischen Incident belaufen sich auf 141.628 USD

Unternehmen mit der längsten MTTD, also der Zeit, die benötigt wird, um einen Incident nach dem ersten Auftreten eines Fehlers zu identifizieren, verzeichnen die höchsten IT-Kosten bei kritischen Incidents (Abbildung 4). Dies zeigt, wie ein Problem zu einem frühen Zeitpunkt im Event Management-Prozess bis hin zum Incident Management eskalieren kann.

Das Incident-Volumen treibt die IT-Kosten in die Höhe: Bei Unternehmen mit den höchsten Incident-Zahlen betragen die IT-Kosten mehr als das Vierfache als bei Unternehmen mit der geringsten Incident-Anzahl. Dies spiegelt sich auch in der Tatsache wider, dass mehr Dubletten und Wiederholungs-Incidents ebenfalls mit höheren IT-Kosten korrelieren (Abbildung 5). Dies spiegelt wiederum ein schlechtes Event und Incident Management wider und zeigt, dass nicht aus einer effektiven Ursachenanalyse gelernt wurde.

Alles, was getan werden kann, um diese Kosten zu senken, sollte willkommen sein. Die in diesem Bericht vorgestellte Untersuchung zeigt, dass eine frühere Erkennung von Incidents und ein effizienterer Incident-Untersuchungsprozess die Auswirkungen von IT Incidents verringern. Zudem ergab die Untersuchung, dass sich durch eine effektive Kernursachenanalyse vermeiden lässt, dass Incidents wiederholt auftreten. All diese Faktoren reduzieren die Kosten von Incidents für die IT und die noch höheren Folgekosten und Schäden für das Unternehmen.

Figure 3: Durchschnittskosten eines kritischen Incidents für IT und das Unternehmen

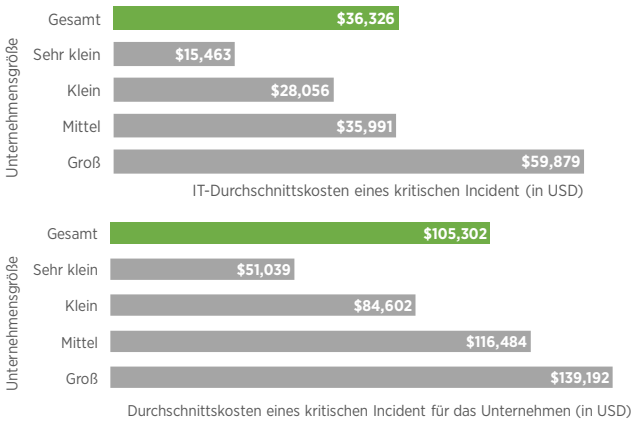


Figure 4: Durchschnittliche Erkennungszeit (Mean Time to Detect, MTTD) und Kosten eines kritischen Incidents für IT

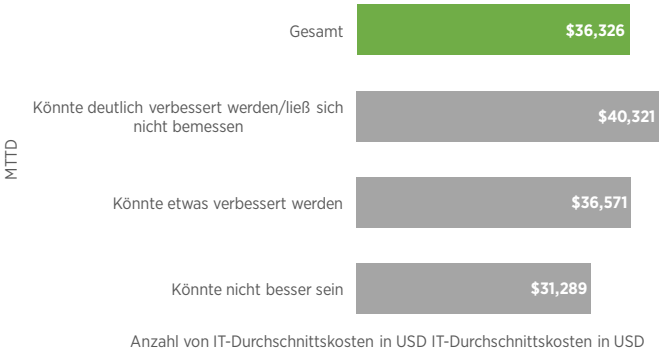
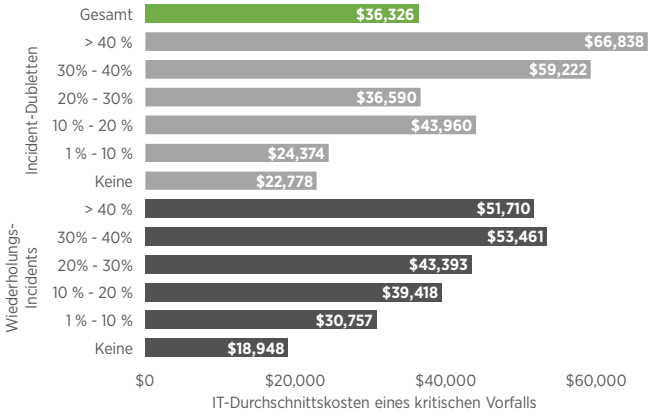


Figure 5: Duplizierung und Wiederholung von Incidents und Kosten kritischer Incidents für die IT



BEHANDLUNG VON INCIDENTS

Incidents können erst behandelt werden, wenn sie erkannt wurden, sei es durch automatisiertes Event Management oder menschliches Reporting, durch IT-Fachleute, Endanwender oder Kunden. 80 % sind der Meinung, dass sie ihre MTTD verbessern könnten, während 20 % glauben, dass ihre MTTD nicht besser sein könnte. Die Zahl derjenigen, die angeben, die von ihren IT-Monitoring-Tools generierte Event-Menge leicht bewältigen zu können, ist dagegen mehr als doppelt so hoch (Abbildung 6).

80 % geben an, sie könnten ihre MTTD verbessern

IT-Teams müssen sicherstellen, dass Incidents entsprechend ihrer Auswirkung auf die Geschäftsprozesse priorisiert werden. Dies setzt voraus, dass IT-Experten über alle Komponenten der IT-Infrastruktur hinweg die notwendige Transparenz und Analytik zur Verfügung stehen.

Nach der Erkennung können der Prozess der Problembehebung und der Abschluss von Incidents in Angriff genommen werden. Die MTTR ist die mittlere Zeit von dem Moment an, in dem ein Incident erkannt wird, bis zu dem Punkt, in dem die Probleme behoben und der Fall abgeschlossen wird. Die MTTR für kritische Incidents ist für viele Unternehmen eine Schlüsselgröße. Die Gesamt-MTTR für kritische Incidents beträgt 5,81 Stunden. Diese wird jedoch durch die Flut der erzeugten Incidents, einschließlich unnötiger Dubletten und Wiederholungen verlängert (Abbildung 7)

Die Gesamt-MTTR für kritische Incidents beträgt 5,81 Stunden

Figure 6: Fähigkeit, Event-Menge zu bewältigen und durchschnittliche Erkennungszeit (Mean Time to Detect, MTTD)

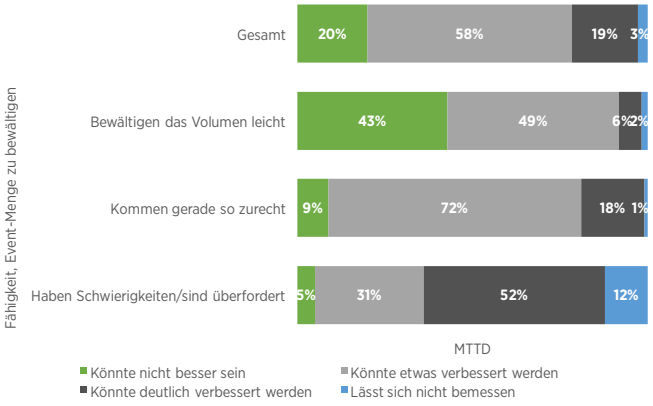
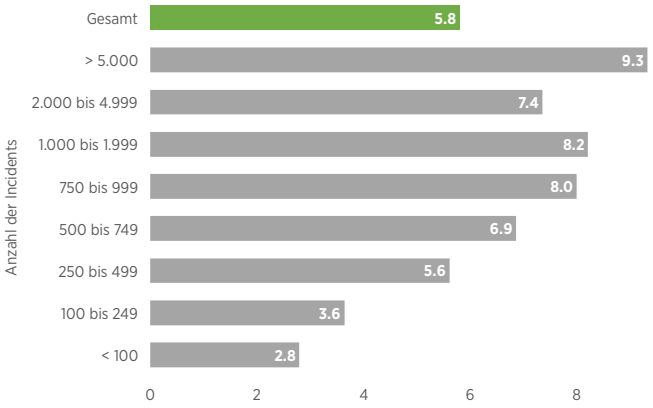


Figure 7: Auswirkung der Incident Menge auf die durchschnittliche Dauer zur Behebung (Mean Time to Repair, MTTR)



Die IT-Teams, die mit größter Wahrscheinlichkeit an der Behebung kritischer Incidents beteiligt sind, stammen in der Regel aus den üblichen Bereichen des IT-Managements (Abbildung 8). IT-Sicherheit steht ganz oben auf der Liste, was nicht verwunderlich ist, da die Sicherheit bei der aktuellen Umfrage als das wichtigste Anliegen des IT-Managements identifiziert wurde (Abbildung 9). Ein Incident ist eher kritisch, wenn es ein Sicherheitsproblem (z. B. einen Denial-of-Service-Angriff oder eine Ransomware-Infektion) oder eine mögliche Sicherheitsverletzung gibt.

Die typische Teamgröße, die zur Behebung eines kritischen Incident eingesetzt wird, wird mit sechs angegeben (Abbildung 10). Dies variiert je nach Unternehmensgröße nur geringfügig, da die Bandbreite der für einen bestimmten Incident erforderlichen Fähigkeiten ähnlich ist. Die Anzahl der Experten, die in den für die Incident-Untersuchung gebildeten Teams gebraucht werden, lässt sich nur schwer reduzieren. Hier kann eine bessere Transparenz der IT-Infrastruktur helfen, da IT-Mitarbeiter damit Zugang zu Daten aus Bereichen der Infrastruktur erhalten, die außerhalb ihres eigenen Zuständigkeitsbereichs liegen.

Figure 8: Involvieren von Entwicklern durch die IT Teams zum Lösen von kritischen Incidents

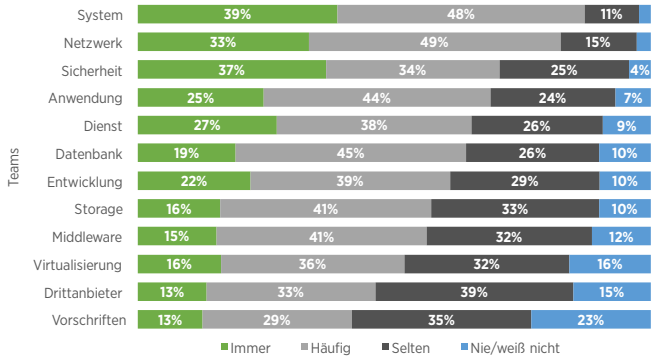
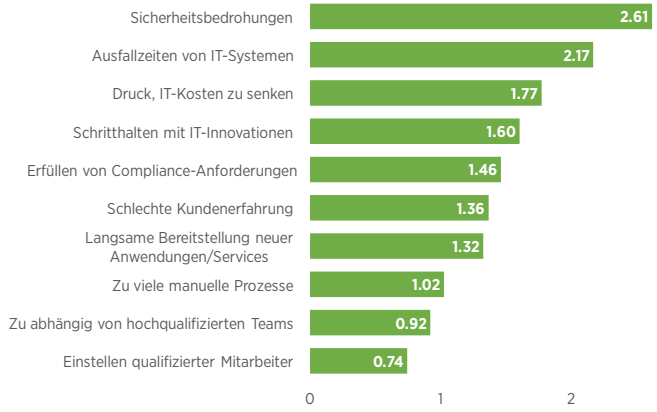


Figure 9: Allgemeine Bedenken des IT Management



EFFEKTIVE KERNURSACHENANALYSE REDUZIERT DIE KOSTEN FÜR KRITISCHE INCIDENTS

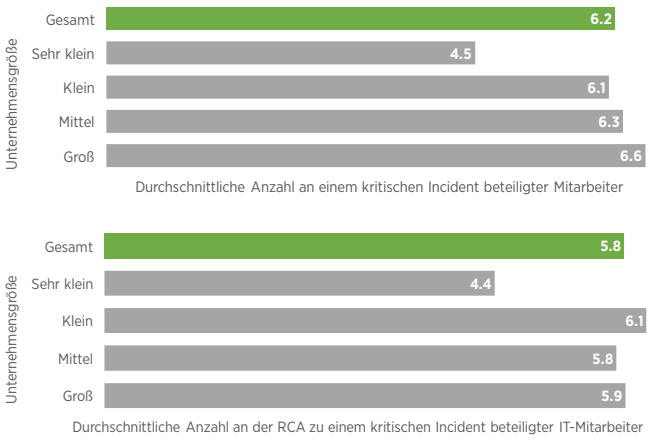
Je schneller ein Incident erkannt und behoben wird, desto schneller kann untersucht werden, was ihn überhaupt verursacht hat. Dies ist die Kernursachenanalyse (Root Cause Analysis, RCA), die unerlässlich ist, um das laufende Management der IT-Infrastruktur zu verbessern und Wiederholungs-Incidents zu vermeiden. Die mittlere Zeit für die Kernursachenanalyse ist 7,23 Stunden, und die RCA wird in 65 % der Fälle durchgeführt. Die durchschnittlich für die RCA gemeldete Teamgröße liegt ebenfalls bei sechs (Abbildung 10).

MDurchschnittlicher Zeitaufwand für die RCA beträgt 7,23 Stunden

Die RCA wird in 65 % der Fälle durchgeführt

Diejenigen, die angeben, die RCA fast immer durchzuführen, weisen nur etwa ein Drittel der Wiederholungs-Incidents im Vergleich zu denjenigen auf, die die Kernursache nur in 50% der Fälle ermitteln. Die Vermeidung von Wiederholungen senkt die Gesamtkosten von IT Incidents.

Figure 10: Einbeziehen von IT Mitarbeitern zum Lösen kritischer Incidents



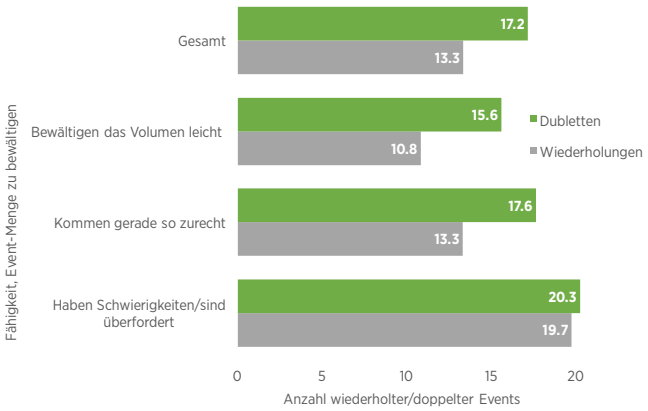
BEWÄLTIGUNG DES EVENT-VOLUMENS UND EVENT MANAGEMENT

Zwei Drittel der Befragten geben an, dass es schwierig ist, die von ihren IT-Monitoring-Tools generierte Event-Flut im Rahmen ihres Event-Management-Prozesses zu bewältigen; 20% haben überhaupt keinen Event-Management-Prozess. 66 % finden die Bewältigung der Event-Mengen anspruchsvoll: 52 % kommen gerade so zurecht, 13 % haben Schwierigkeiten mit der Event-Flut und 1 % sind überfordert damit.

66 % finden die Bewältigung der Event-Mengen anspruchsvoll: 52 % kommen gerade so zurecht, 13 % haben Schwierigkeiten mit der Event-Flut und 1 % sind überfordert damit

Bei denjenigen, die das Event-Volumen im Griff haben, gibt es weniger Dubletten und Wiederholungs-Incidents (Abbildung 11). Dies liegt zum Großteil an den Fähigkeiten von Event Management-Prozessen und den zugehörigen Tools, wie etwa der Fähigkeit, ein Event durch gute Transparenz der IT-Infrastruktur effizient zu sichten. Schlechtes Event-Management führt zu Fehlalarmen, belastet den nachgelagerten Incident Management-Prozess und verzögert die Erkennung und Behebung von Problemen.

Figure 11: Fähigkeit, Event-Menge zu bewältigen und Reduzierung der Duplizierung oder Wiederholung von Incidents



UNNÖTIGE INCIDENTS

Schlechte End-to-End-Sichtbarkeit und Komplexität der IT-Infrastruktur führen zu Incident-Dubletten: Dasselbe Problem wird von einem Service Desk mehrfach protokolliert, und schlimmstenfalls kümmern sich getrennte IT-Teams parallel um den gleichen Incident. 97% der Befragten geben an, dass es bei ihnen Incident-Dubletten gibt, und fast ein Fünftel (17,2%) aller Incidents sind Dubletten.

97% der Befragten geben an, dass es bei ihnen Incident-Dubletten gibt; 17,2% aller Incidents sind Dubletten

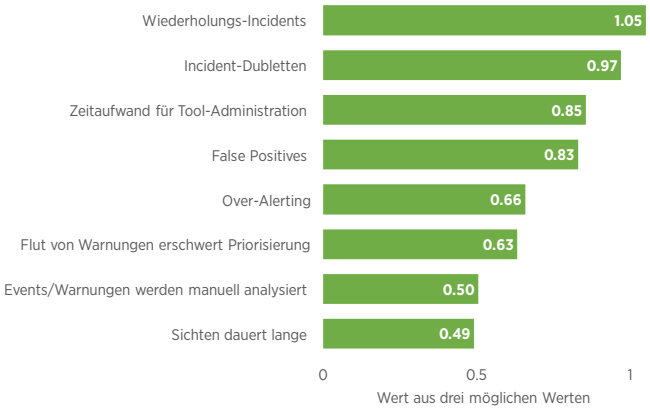
Nach der Behandlung der kurzfristigen Krise, die ein Incident auslöst, kann eine ineffektive Kernursachenanalyse dazu führen, dass sich derselbe Incident später wiederholt, da man nicht aus den vergangenen Problemen gelernt hat. 96% geben an, dass es zu Wiederholungs-Incidents führt, wenn man nicht aus früheren Incidents lernt; 13,3% aller Incidents sind Wiederholungs-Incidents.

96% geben an, dass es zu Wiederholungs-Incidents führt, wenn man nicht aus früheren Incidents lernt; 13,3% aller Incidents sind Wiederholungs-Incidents

Die Menge an Doppel- und Wiederholungs-Incidents sollte nicht unterschätzt werden. Bei einem durchschnittlich großen Unternehmen kann man von 374 unnötigen (Dubletten) oder vermeidbaren (Wiederholungen) Incidents ausgehen, bei großen Unternehmen sind es gar 852. Die Ursachen für diese unnötige IT-Arbeit und die damit verbundenen Kosten liegen in Problemen bei den Event und Incident Managementprozessen.

IT-Management-Teams sind sich dessen bewusst: Bei den Auswirkungen verschiedener Probleme auf die Effizienz der IT-Abläufe stehen Incident-Dubletten und Wiederholungs-Incidents ganz oben auf der Liste (Abbildung 12). Wenn man dieses Problem behebt, lässt sich damit etwa ein Drittel der protokollierten IT Incidents vermeiden (plus der Zeitaufwand für ihre Untersuchung).

Figure 12: Die Auswirkungen, die Probleme auf die Effizienz von IT Operations haben



TRANSPARENZ DER IT-INFRASTRUKTUR

Tools, die eine gute Transparenz der IT-Infrastruktur gewährleisten, führen zu einer schnelleren Erkennung und Untersuchung von Incidents und verbessern die Ursachenanalyse. Die Umsetzung variiert jedoch: Die holistische End-to-End-Transparenz von IT-Prozessen schnitt am schlechtesten ab: Nur 45 % der Teilnehmer gaben an, dass ihre Transparenz ausgezeichnet oder gut sei (Abbildung 13).

Die Transparenz ist in traditionellen Bereichen wie Servern, Storage und Netzwerken tendenziell besser und bei Technologien der nächsten Generation wie Cloud Computing, Containern und Mobilität eher schlechter. Dies deutet darauf hin, dass die Monitoring-Möglichkeiten nicht mit dem Tempo der Veränderungen Schritt gehalten haben, die zur Erfüllung der Unternehmensanforderungen notwendig sind. Schlechte Transparenz in Bezug auf die holistische Bereitstellung von IT und die Endanwender-Erfahrung erschwert es, die Hauptsorge im Hinblick auf die potenziellen Folgen von IT Incidents anzugehen: Kunden- und Anwendererfahrung.

Die Bewertungen in Abbildung 13 können verwendet werden, um eine Gesamtsichtbarkeitsbewertung zu berechnen (siehe Anhang zur Berechnung). Bei einem Maximalwert von 4 beträgt die durchschnittliche Sichtbarkeit 2,56 – da ist also noch viel Luft nach oben. Nur 2,5 % haben volle Transparenz über die gesamte relevante Infrastruktur hinweg, während 0,7 % angeben, keine Sichtbarkeit zu haben.

Nur 2,5 % haben volle Transparenz über die gesamte relevante Infrastruktur hinweg, während 0,7 % angeben, keine Sichtbarkeit zu haben

In durchschnittlichen Unternehmen gibt es 19,8 Monitoring-Tools, in großen Unternehmen möglicherweise Hunderte. Bessere Sichtbarkeit durch effektives Monitoring sollte die Zahl der blinden Flecken reduzieren, 80 % der Befragten geben jedoch zu, dass es bei ihnen blinde Flecken gibt.

Bessere Sichtbarkeit korreliert mit weniger Dubletten und Wiederholungs-Incidents. Dies geschieht meist indirekt durch die Verbesserung des Gesamtprozesses zur Incidents-Erkennung (Abbildung 14). Auch die Zahl der Wiederholungen wird voraussichtlich abnehmen, da IT-Mitarbeiter mehr Zeit haben, die Ursachen von Incidents zu untersuchen, aus Fehlern zu lernen und Wiederholungen zu verhindern.

Figure 13: Transparenz in die IT-Infrastruktur

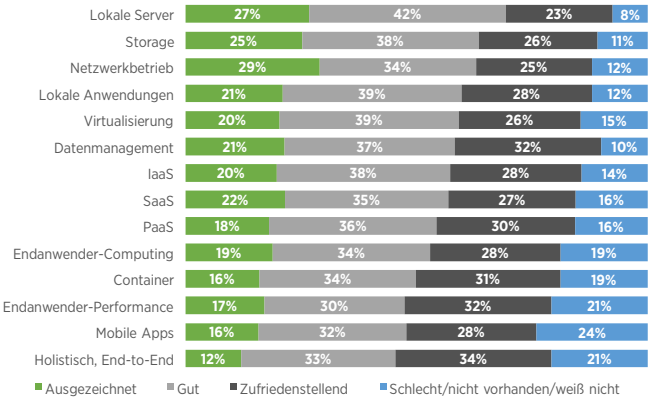
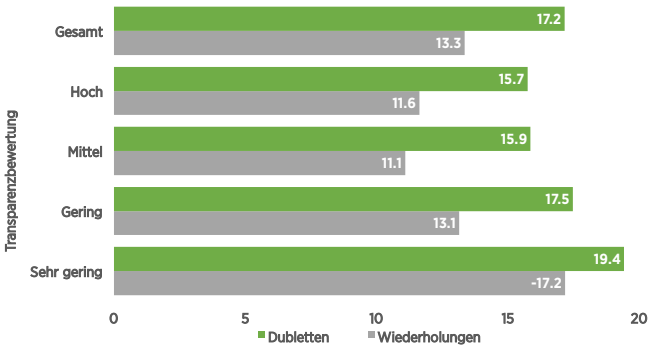
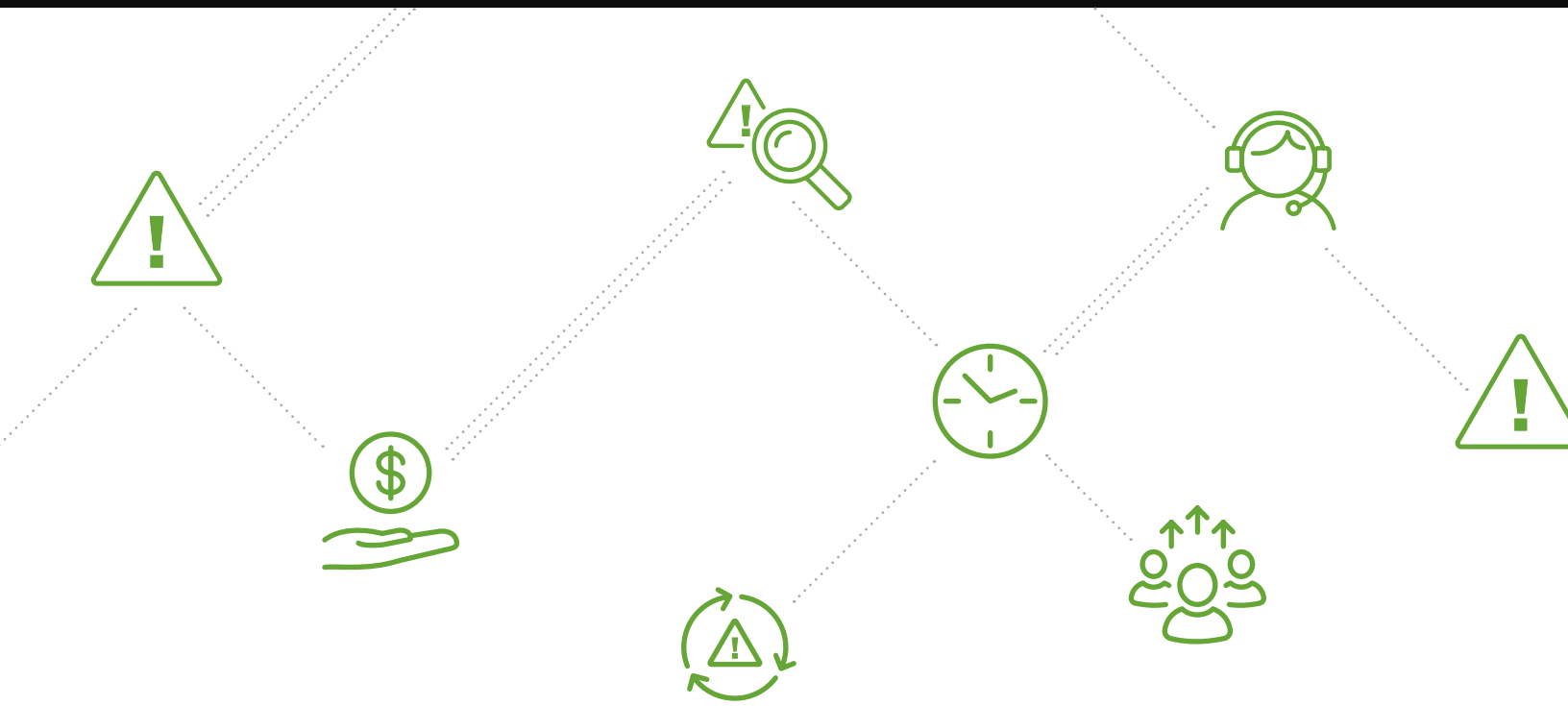


Figure 14: Transparenz und Wiederholung / Duplizierung von Incidents





FAZIT

IT-Abteilungen stehen unter dem Druck, die Entwicklung qualitativ hochwertiger digitaler Services für Anwender und Kunden zu beschleunigen, um wettbewerbsfähig zu bleiben. Dies muss bei kontrollierten IT-Kosten erreicht werden.

Die steigende Komplexität von IT-Umgebungen führt dazu, dass IT-Mitarbeiter sich schwer tun, Incidents effektiv zu verwalten, was die Kosten sowohl für die IT-Abteilung als auch für das zugehörige Unternehmen unnötig erhöht. In einer Welt, die zunehmend auf digital gesteuerte Prozesse angewiesen ist, werden mehr Benutzer und Kunden davon betroffen sein, wenn der Managementprozess für IT Incidents nicht verbessert wird. Dies erhöht wiederum das Risiko von Reputationsschäden.

Die Behandlung kritischer IT Incidents muss eines der wichtigsten IT-Ziele sein. IT-Teams sollten mit Tools ausgestattet werden, die die End-to-End-Transparenz der Prozesse und ihrer zugrundeliegenden IT-Infrastruktur ermöglichen. Die Tools werden benötigt, um IT Incidents schnell zu erkennen und zu untersuchen, die Kernursachenanalyse zu optimieren und die Größe der Problembehebungs-Teams zu reduzieren. All dies reduziert die IT-Kosten sowie die deutlich höheren Folgekosten und Auswirkungen von IT Incidents für Unternehmen.

Klicken Sie HIER, um die Kosten kritischer IT Incidents für Ihr Unternehmen zu berechnen.

ANHANG

Berechnung der Werte in den Abbildungen 1, 9 und 12

Bei bestimmten Fragen wurden die Teilnehmer gebeten, die drei oder fünf für sie wichtigsten Probleme aus Problemvorschlägen auszuwählen, wobei zuerst das wichtigste, dann das zweitwichtigste usw. gewählt wurden, bis die Auswahl drei (bzw. fünf) Probleme umfasste. Bei der Analyse wurde jeder Auswahl nach folgendem Schema ein Wert zugeordnet:

Fünf Probleme (Abbildungen 1 und 9)

- Wert = 5 für wichtigstes Problem
- Wert = 4 für zweitwichtigstes Problem
- Wert = 3 für drittwichtigstes Problem
- Wert = 2 für viertwichtigstes Problem
- Wert = 1 für fünftwichtigstes Problem
- Wert = 0 für jedes der nicht ausgewählten Probleme

Drei Probleme (Abbildung 12)

- Wert = 3 für wichtigstes Problem
- Wert = 2 für zweitwichtigstes Problem
- Wert = 1 für drittwichtigstes Problem
- Wert = 0 für jedes der nicht ausgewählten Probleme

Anhand dieser Werte wurde die gewichtete durchschnittliche Besorgnis im Zusammenhang mit den im Bericht verwendeten Problemen berechnet. Da jeder Befragte fünf (oder drei) Probleme in der Reihenfolge ihrer Wichtigkeit auswählen soll, muss ein Problem in der Skala der Wichtigkeit fallen, wenn ein anderes steigt.

Aus Daten in Abbildung 13 berechneter Transparenzwert

Die Gesamtpunktzahl für die Sichtbarkeit der Infrastruktur, die sich aus den Daten in Abbildung 13 ergibt, wurde berechnet, indem 4 Punkte für ausgezeichnet, 3 für gut, 2 für zufriedenstellend, 1 für schlecht und 0 für nicht vorhanden/weiß nicht vergeben wurden und dann ein Gesamtdurchschnitt berechnet wurde.

Wechselkurse

Die relevanten Finanzdaten werden in USD angegeben. Bei der Befragung wurde jedoch die jeweilige Landeswährung verwendet. Dabei wurden die folgenden Wechselkurse zugrunde gelegt: 1,00 US-Dollar =

- 1,36 Singapur-Dollar
- 112 japanische Yen
- 1,28 australische Dollar
- 8,05 schwedische Kronen
- 0,85 Euro
- 0,76 britische Pfund

Demographics

Alle Teilnehmer der Umfrage waren leitende IT-Manager. Nachfolgend sind die teilnehmenden Länder und Wirtschaftszweige nach Unternehmensgröße gegliedert dargestellt. Die Feldarbeit wurde von Quocircas Forschungspartner Vanson Bourne durchgeführt.

DEMOGRAPHICS

Alle Teilnehmer der Umfrage waren leitende IT-Manager. Nachfolgend sind die teilnehmenden Länder und Wirtschaftszweige nach Unternehmensgröße gegliedert dargestellt. Die Feldarbeit wurde von Quocircas Forschungspartner Vanson Bourne durchgeführt.

Figure 15: Länder nach Unternehmensgröße

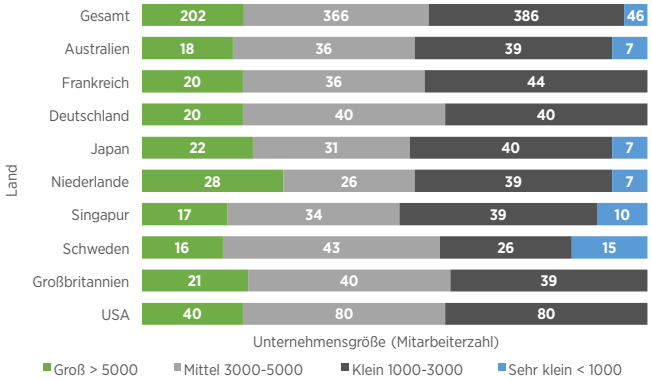
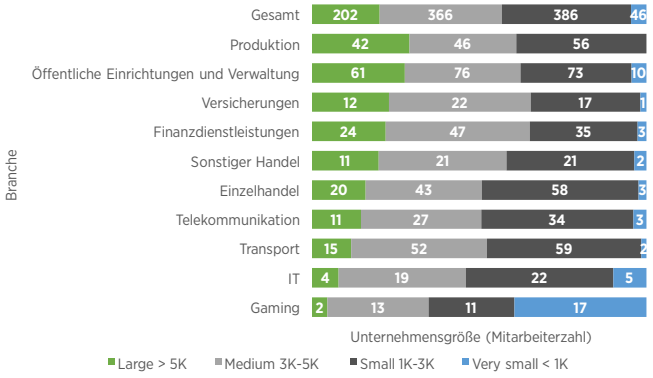


Figure 16: Unternehmensbereiche nach Unternehmensgröße



splunk>

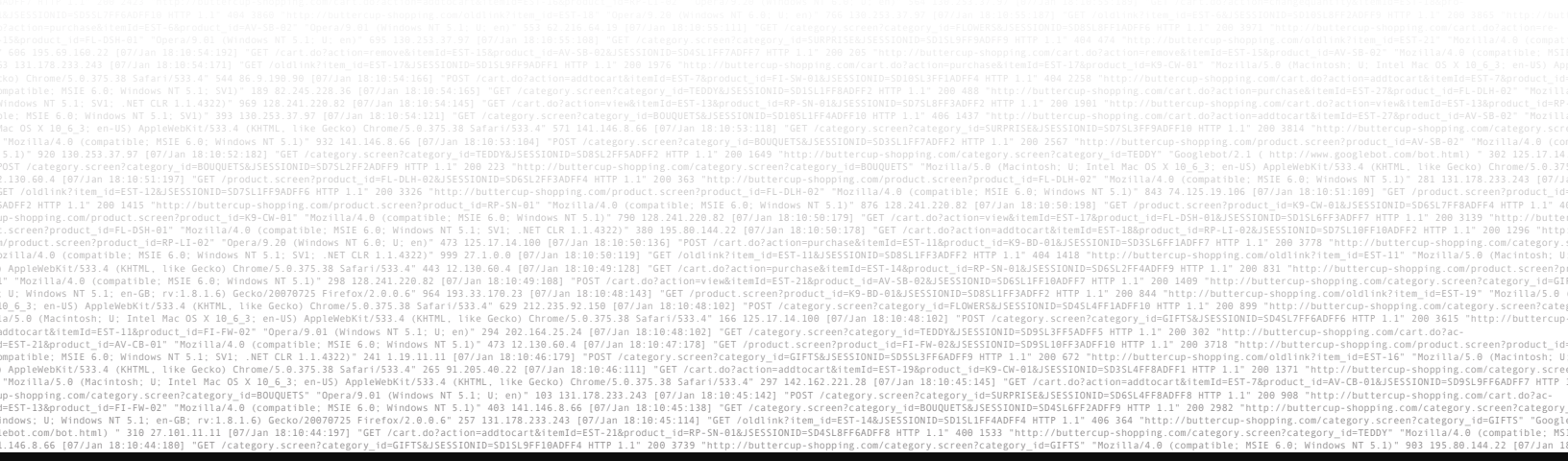
ÜBER SPLUNK

Splunk Inc. (NASDAQ: SPLK) verwandelt Maschinendaten in Antworten. Unternehmen nutzen die branchenführenden Splunk-Lösungen mit integriertem Machine Learning zur Lösung ihrer größten Herausforderungen in den Bereichen IT, Internet of Things und Sicherheit. Schließen Sie sich den Millionen passionierter Nutzer an und entdecken Sie noch heute Ihr „Aha“-Erlebnis mit Splunk: http://www.splunk.com.

quocirca

ÜBER QUOCIRCA

Quocirca ist ein Unternehmen für Marktforschung und Marktanalyse mit Sitz in Großbritannien. Quocirca erstellt frei verfügbare Inhalte, deren Zielgruppe IT-Entscheidungsträger und Influencer sind. Ein Großteil der von Quocirca produzierten Inhalte basiert auf Primärforschung in Europa, Amerika und Asien, die von einem breiten Spektrum von Unternehmen der IT-Branche gesponsert wird. Quocirca-Inhalte werden von einem unabhängigen Standpunkt aus verfasst und beziehen sich auf den IT-Einsatz im Unternehmenskontext und nicht auf bestimmte Produkte. Durch die engen Beziehungen zu den Medien erreichen Quocirca Artikel und Berichte Millionen von Entscheidungsträgern und Influencern: www.quocirca.com.



splunk> | quocirca Learn more: www.splunk.com/asksales www.splunk.com

WP-Splunk-Quocirca-Cost-of-Critical-IT-Incidents-101 GERMAN