Die versteckten Kosten von Ausfallzeiten

Die Global 2000 haben ein
400-Milliarden-Dollar-Problem

splunk>

Geschäftsunterbrechungen sind unvermeidlich. Doch die erfolgreichsten Unternehmen der Gegenwart sind in der Lage, adaptiv auf Systemstressoren zu reagieren und sich schnell wieder zu fangen, weil sie in ein solides Fundament für digitale Resilienz investieren. Ungeplante Ausfallzeiten stellen diese Resilienz jedoch immer wieder auf die Probe und fordern in vielen Fällen einen hohen Tribut.

Die tatsächlichen finanziellen Auswirkungen und die Art der Ausfallzeiten sind schwer zu bestimmen. Die Forschung beschränkt sich oft auf Ausfälle aufgrund von IT-Problemen. Übersehen werden dabei Incidents, die durch Schwächen der Cybersicherheit entstehen. Und auch die nachgelagerten wirtschaftlichen Auswirkungen bleiben meist ganz außer Acht. Mit einem derart unvollständigen Bild wollten wir uns nicht zufriedengeben.

In Zusammenarbeit mit dem internationalen Wirtschaftsinstitut Oxford Economics konnten wir die Gesamtkosten von Ausfallzeiten der Global 2000 auf $ 400 Milliarden pro Jahr beziffern. Heißt: Jedes dieser Unternehmen verliert im Schnitt $ 200 Millionen pro Jahr, weil ihre digitalen Umgebungen unerwartet ausfallen.

Es zeigt sich auch, dass dies nur die Spitze des Eisbergs ist. Hinzu kommen weitere, versteckte Kosten in noch größerem Umfang – etwa milliardenschwere Auswirkungen auf den Börsenwert. Die Daten bestätigen auch den Verdacht, den wir schon lange hegen: Probleme sowohl bei der Cybersicherheit als auch bei Infrastruktur bzw. Anwendungen sind Ursachen für Ausfallzeiten.

Ich freue mich, Ihnen nun den Bericht „Die versteckten Kosten von Ausfallzeiten“ vorstellen zu können, der erstmals die direkten und die früher übersehenen Kosten ungeplanter Ausfallzeiten untersucht, die häufigsten Ursachen aufzeigt und erklärt, wie es resilienten Unternehmen gelingt, die Folgen von Downtime minimal zu halten.

Das Fazit fällt eindeutig aus: Angesichts der finanziellen Folgen von Ausfallzeiten muss digitale Resilienz eine Top-Priorität für Geschäfts- und Technologieverantwortliche werden – ohne Ausnahme. Es ist absolut notwendig, dass das Management begreift, welche Folgen Ausfallzeiten für den Unternehmenserfolg haben, und die notwendigen Schritte in Richtung umfassender digitaler Resilienz unternimmt.

Gary Steele
President, Go-to-Market, Cisco
GM, Splunk

Die Folgekosten von Ausfallzeiten

„Multinationales Telekommunikationsunternehmen erleidet weltweiten Systemausfall“ oder „Cyberangriff: Krankenhaus sagt Operationen ab, Patientendaten in den Händen von Hackern“ – solche Schlagzeilen lesen wir gefühlt jede Woche. Die Begleitmusik dazu: verzweifelte PR-Schadensbegrenzung, Aufregung in den sozialen Medien und ein heftiger Kurseinbruch.

Ungeplante Ausfallzeiten[1] (also jede Beeinträchtigung bzw. jeder Ausfall eines Business-Systems) können aufseiten der Kundschaft als lästiges Ärgernis erscheinen – oder sogar als Gefahr für Leib und Leben. Für Unternehmen bedeuten Ausfallzeiten einen handfesten finanziellen Schaden: in Form von Bußgeldern, Umsatzverlusten, Überstunden und vielem mehr.

Da kommt einiges zusammen.

Wir haben 2.000 Führungskräfte der Global 2000[2] befragt und mit Unterstützung von Oxford Economics durchschnittliche Kosten von Ausfallzeiten in Höhe von $ 400 Milliarden pro Jahr errechnet. Das entspricht $ 200 Millionen pro Unternehmen oder ca. 9 % des Gewinns,[3] was in jeder Hinsicht erheblich ist.

Und das sind nur die direkten Kosten. Die versteckten Kosten können ebenfalls gewaltig auf die Bilanz durchschlagen. Wir sprechen hier von Aktienkursen im Sinkflug. Von verzögerten Markteinführungen, während der Wettbewerb mit der Zielgruppe davonzieht. Von Marken, die ihre Reputation einbüßen, sodass sich Investoren und Kundschaft abwenden. Die Liste lässt sich noch fortsetzen.

Es liegt auf der Hand, dass sich diese und andere versteckte Kosten bei einem einzelnen Unternehmen leicht auf mehr als $ 200 Millionen jährlich belaufen können. Und unsere Untersuchung zeigt, dass Unternehmen für diese Auswirkungen noch lange nach Wiederherstellung der Systeme bezahlen, und zwar über Monate hinweg.

Wir haben auch die Ursachen von Ausfallzeiten untersucht und stellen fest, dass diese ebenso häufig auf Cybersicherheitsprobleme wie auf Infrastruktur- bzw. Anwendungsprobleme zurückzuführen sind. Wirksame Abhilfestrategien müssten also beide Bereiche berücksichtigen. Tatsächlich zeigen die Daten, dass die Unternehmen, die einen solchen Ansatz verfolgen, in der Spitzengruppe zu finden sind: Sie sind resilienter als die Mehrheit, und sie haben weniger unter Ausfällen und deren Folgen zu leiden.

Sehen wir uns das genauer an.

1 Für die Studie wurde Ausfallzeit (Downtime) als jederlei Beeinträchtigung von Services (z. B. Latenzen/Verzögerungen) sowie Nichtverfügbarkeit von Services in Bezug auf die End-User kritischer Geschäftssysteme definiert.

2 „Die Global 2000 listen die größten Unternehmen der Welt auf, und zwar anhand von vier Kriterien: Umsatz, Gewinn, Vermögen und Marktwert.“ (Forbes)

3 Bezogen auf die summierten Global-2000-Gewinne in Höhe von $ 4,4 Billionen (Andrea Murphy, Hank Tucker: The Global 2000. In: Forbes, 8. 6. 2023).

Inhalt

Ausfallzeiten werfen noch mehr Kosten auf

„Wenn Sie sich die Kosten von Ausfallzeiten ansehen, dann ist das ein erheblicher Betrag. Denn unter Umständen sitzen da 15 technische Fachleute in gehobener Position mit einem Stundenlohn von x um einen Tisch und versuchen herauszufinden, woran es hakt. Was sollen wir tun? Wie gehen wir mit dem Kollateralschaden um? Wie gehen wir mit der Kundschaft um? Wie gehen wir mit den Aufsichtsbehörden um?“

— Chris Russell Miller, Head of IT and Cyber Risk, BNP Paribas Personal Finance UK

Die direkten Downtime-Kosten im Einzelnen

Die wirtschaftlichen Folgen von Ausfallzeiten beschränken sich nicht auf einzelne Abteilungen oder Kostenkategorien. Weil wir ein Gesamtbild wollten, haben wir Finanzvorstände und Chief Marketing Officers befragt, die Auskunft über die weiteren Auswirkungen verschlechterter digitaler Erfahrungen auf Markenwert und Finanzen geben können, außerdem Security-, IT-Operations- und Engineering-Fachleute. Wir wollten von den Befragten anhand von mehreren Dimensionen wissen, wie hoch die Kosten von Ausfallzeiten sind. In jedem Fall ist klar, dass Ausfallzeiten kein rein technisches, sondern ein betriebswirtschaftliches Problem sind.

Auf Basis der Befragungsergebnisse hat Oxford Economics berechnet, dass Ausfallzeiten die Global-2000-Unternehmen $ 400 Milliarden pro Jahr kosten. Das sind $ 200 Millionen pro Unternehmen und Jahr – also etwa 9 % des Gewinns. Jede Minute Ausfallzeit kostet im Durchschnitt $ 9.000. Das sind $ 540.000 pro Stunde.

Wie kommen diese Zahlen zustande? Schlüsseln wir sie auf.

Die Umsatzverluste stehen bei den direkten Kosten mit $ 49 Millionen pro Jahr an erster Stelle, sie machen mehr als doppelt so viel aus wie der zweitgrößte Posten. Das tut natürlich weh. Für 61 % der Befragten sind diese Verluste „sehr“ hoch oder „untragbar“ hoch. Laut den befragten CFOs dauert es im Schnitt 75 Tage, bis sich die Erlöse wieder erholen.

Die direkten Kosten von Ausfallzeiten schmälern das Geschäftsergebnis

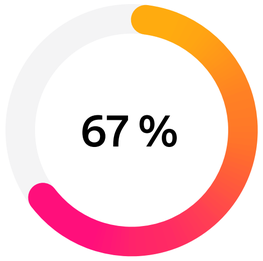
Umsatzverluste machen den bei Weitem größten Einzelposten aus, aber auch die anderen direkten Kosten summieren sich.

Beträge sind auf ganze Zahlen gerundet.

Bußgelder stehen an zweiter Stelle der direkten Kosten, sie belaufen sich auf durchschnittlich $ 22 Millionen pro Jahr. 79 % der befragten Technologie-Führungskräfte bestätigen, dass im Wirtschaftsraum ihres Unternehmens strenge Vorgaben für Ausfallzeiten gelten – für den Finanzsektor etwa die europäische Verordnung (EU) 2022/2554, besser bekannt als Digital Operational Resilience Act (DORA). Angesichts der zunehmenden Regulierung ist Resilienz eine entscheidende Compliance-Grundlage für Unternehmen, die sich die zum Teil saftigen Geldbußen ersparen wollen.

Wie schlagen Ausfallzeiten sonst noch auf die Bilanz durch? Den Marketing-Verantwortlichen zufolge geben Unternehmen im Durchschnitt $ 14 Millionen für Kampagnen aus, um die Reputation der Marke zu reparieren – und noch einmal $ 13 Millionen für Öffentlichkeitsarbeit und die Beziehungen zu Investoren und Behörden. Den CMOs (Chief Marketing Officers) ist durchaus bewusst, wie relevant Ausfallzeiten für ihre Arbeit sind: 72 % sagen, dass die Minimierung von Ausfallzeiten „wichtig“ oder „sehr wichtig“ für ihre Rolle ist.

Cyberangriffe gehen direkt ins Geld. 67 % der befragten CFOs (Chief Financial Officers) geben an, dass sie CEO und Vorstand bei einem Ransomware-Angriff in der Regel zur Zahlung des Lösegelds raten, entweder direkt, über eine Versicherung, eine Drittpartei oder – was am häufigsten vorkommt – in einer Kombination dieser drei Möglichkeiten. Die Zahlungen von Ransomware-Lösegeldern ($ 11 Millionen) und für Cyber-Erpressung bei Ransomware-Angriffen ($ 8 Millionen) summieren sich mittlerweile auf $ 19 Millionen pro Jahr.

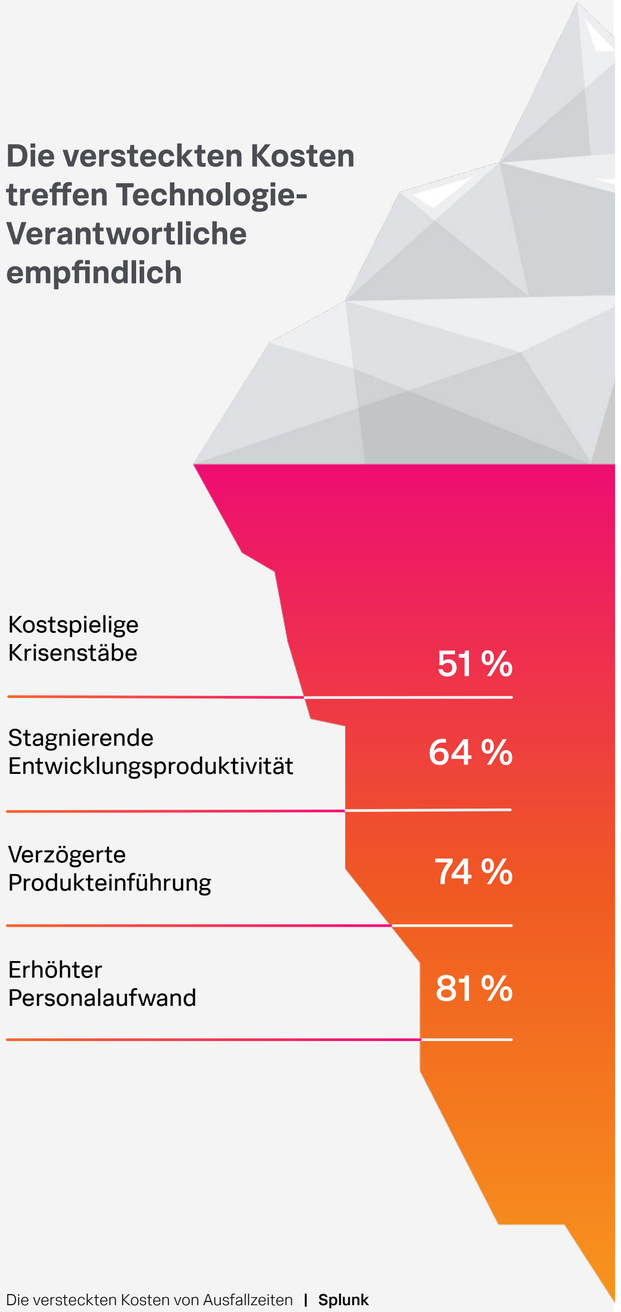


der CFOs raten CEO und Vorstand dazu, das Lösegeld zu zahlen

Egal wie hoch Ihre Gewinnspanne ist, Sie müssen davon die Kosten von Ausfallzeiten abziehen. Ihnen entgeht Umsatz. Und wenn das zum Dauerzustand wird, verlieren Sie Ihren Ruf und müssen dauerhaft mit Gewinneinbußen rechnen.

— Mauli Tikkiwal, IT Director und Vorstandsmitglied eines multinationalen Fertigungsunternehmens

Die versteckten Kosten treffen Technologie-Verantwortliche empfindlich



Versteckte Kosten von Ausfallzeiten sind beachtlich

Die versteckten Kosten von Ausfallzeiten sind im Vergleich schwerer zu messen und weniger sichtbar, wirken sich deshalb aber nicht weniger heftig aus als die direkten Kosten. Ausfälle erzeugen eine Flutwelle von Nachwirkungen, die jeden Winkel des Unternehmens erreicht. Security-, ITOps- und Engineering-Teams irren im Labyrinth der Fehler-Ursachen-Analyse umher, CMOs schwenken Marketing und Kommunikation auf das Krisenmanagement um, und die CFOs müssen live zusehen, wie die Aktienkurse einbrechen.

Wenn es zu Ausfällen kommt, müssen ganze Teams die Arbeit an wertschöpfenden Projekten (wie der Einführung neuer digitaler Produkte und Erfahrungen) liegen lassen und stattdessen Software-Patches aufspielen und Post-Mortem-Analysen durchführen. Wer das schon einmal erlebt hat, weiß, dass bei einem Incident alle in Konferenzschaltung sind – und bis das Problem gelöst ist, geht niemand nach Hause. Die Produktivität sinkt, Innovationen werden zurückgestellt und Produkteinführungen müssen warten.

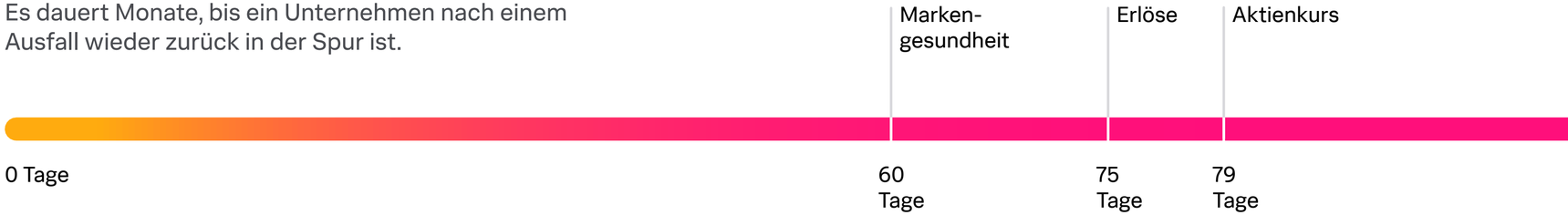
Das alles schadet der Position im Wettbewerb und dürfte insgesamt Kosten in zweistelliger Millionenhöhe aufwerfen.

Ein weiterer Grund zur Sorge sind die persönlichen Risiken, die mit Ausfallzeiten einhergehen. 39 % der Befragten aus dem Technologiebereich befürchten, persönlich für einen Incident haftbar gemacht zu werden, weitere 38 % machen sich Sorgen, dass Ausfälle sich auf ihre Leistungsbeurteilung auswirken – oder sogar zur Kündigung führen.

Die wohl heftigsten versteckten Kosten? 28 % aller Befragten geben an, dass durch Ausfallzeiten der Unternehmenswert leidet. Schon bei einem einzigen Ausfall müssen Unternehmen damit rechnen, dass der Aktienkurs um 1 % bis 9 % sinkt (Mittelwert: 2,5 %). Im Durchschnitt dauert es dann 79 Tage, bis er sich wieder erholt. Das tut weh.

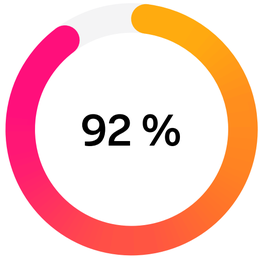
Der lange Weg zurück in die Normalität

Es dauert Monate, bis ein Unternehmen nach einem Ausfall wieder zurück in der Spur ist.



Durch Ausfallzeiten sinkt der Kundenwert

Es sieht nie gut aus, wenn die Kundschaft mehr über Ihre digitale Experience weiß als Sie selbst. Dennoch müssen 41 % der technischen Führungskräfte zugeben, dass Ausfallzeiten „oft“ oder sogar „immer“ als Erstes von der Kundschaft bemerkt werden. Und wenn ein Incident in den sozialen Medien für Aufregung sorgt, kann dies die Customer Experience zerstören, die Kundentreue lässt nach und die öffentliche Wahrnehmung des Unternehmens leidet. 40 % der CMOs sagen, dass durch Ausfälle der durchschnittliche Customer Lifetime Value (CLV) sinkt, ebenfalls 40 % geben zu Protokoll, dass Ausfallzeiten den Beziehungen zu Resellern und/oder Partnern schaden.



der CMOs sagen, dass Ausfallzeiten die Position der Marketing-Abteilung im Wettbewerb schwächen

29 % der Befragten haben aufgrund von Ausfallzeiten bereits Kundschaft verloren, 44 % sagen, dass Ausfallzeiten den Ruf des Unternehmens beschädigen. Den CMOs zufolge dauert es im Durchschnitt 60 Tage, bis sich das Marken-Image nach der Behebung eines Incidents wieder erholt hat.

Die Auswirkungen von Ausfallzeiten auf Kundentreue und Reputation sind nicht von der Hand zu weisen. Die Marketing-Verantwortlichen müssen rasch handeln, damit ihnen die Felle nicht davonschwimmen.

Reputationsschäden, Net Promoter Scores und Social-Media-Posts sind natürlich – wie bei allen Systemstörungen – die Kollateralschäden dieser Art von Incidents.

— Chris Russell Miller, Head of IT and Cyber Risk, BNP Paribas Personal Finance UK

Die nachgelagerten Auswirkungen von Ausfallzeiten auf das Marketing

67%
Mehr für Werbekampagnen zur Wiederherstellung der Marke aufgewendet

67%
Teams für das Krisenmanagement abgestellt

65%
Mindestens einmal in den Nachrichten genannt (national oder international)

62%
Marketing- und Sales-Produktivität verloren

61%
Budget zum Krisenmanagement umgeschichtet

Ausfallursachen gibt es überall

„Wer Lehrgeld für Cybersecurity-Ausfälle zahlen muss, hat die teuerste Downtime-Variante kennengelernt.“

— Luca Panattoni, Head of IT and Digital Transformation, Carrefour

Ausfallzeiten sind nicht nur ein Problem von ITOps oder Engineering. Die Ursachen von Ausfallzeiten liegen auch in der Security. Unternehmen sollten sich die häufigsten Auslöser bewusst machen und die Incident-Reaktion entsprechend ausrichten, damit sie nicht kalt erwischt werden. Unsere Befragung bestätigt, dass Ausfallzeiten zweierlei Ursachen haben: 56 % davon sind auf Security Incidents wie Phishing-Angriffe zurückzuführen, 44 % auf Infrastruktur- oder Anwendungsprobleme wie Softwarefehler. In beiden Fällen spielt menschliches Versagen eine entscheidende Rolle. Diese Bedrohung ist am schwierigsten zu erkennen und zu beseitigen.

Die meisten Einzelsysteme haben zwar eine Verfügbarkeit von 99 und noch weiteren Neunen, doch bei Hunderten bis Tausenden von Systemen summieren sich die Ausfallzeiten. Im Durchschnitt verzeichnet ein Global-2000-Unternehmen 466 Stunden Ausfallzeit aufgrund von Cybersecurity Incidents und 456 Stunden Ausfallzeit, die auf Anwendungen oder Infrastruktur zurückzuführen sind.

Cyberangriffe passieren meist dann, wenn sich Technologien weiterentwickeln und man auf die neuen Bedrohungen, die daraus für das Unternehmen entstehen, nicht gefasst ist.

— Mauli Tikkiwal, IT Director und Vorstandsmitglied eines multinationalen Fertigungsunternehmens

Ausfälle entstehen aus Fehlern von Menschen

Die Hauptursache von Ausfallzeiten ist menschliches Versagen, z. B. in Form von Fehlkonfigurationen von Software oder Infrastruktur. Die Hälfte der Befragten gibt an, dass dies „oft“ oder „sehr oft“ der Fall sei. Solche Fehler können zu Performance-Problemen führen, die ganze Systeme zum Absturz bringen oder die Sicherheit des Unternehmens gefährden.

Wenn Menschen Fehler machen, dauern auch Erkennung und Behebung am längsten. Im Durchschnitt vergehen 17 - 18 Stunden, bis der Incident bemerkt wird. Dann dauert es noch weitere 67 - 76 Stunden, bis die durch menschliches Versagen verursachten Ausfälle und Leistungseinbußen bei Services (z. B. Latenzen) behoben sind. Es ist durchaus normal, dass die Systeme mehrere Tage nur langsam und mit Verzögerungen arbeiten.

Security: Gleich an zweiter Stelle nennen die befragten Sicherheitsfachleute Malware- und Phishing-Angriffe als die häufigsten Ursachen von Ausfallzeiten. Sie geben außerdem zu bedenken, dass die Problemlösung in seltenen Einzelfällen deutlich länger dauert. Zero-Day-Exploits z. B. sind Angriffe auf bislang unbekannte Schwachstellen, über die sich Angreifer erstmals Zugang zu den Systemen verschaffen. Entsprechend länger dauern Erkennung und Wiederherstellung, weil schwer zu eruieren ist, was genau geschehen ist, und weil es für diese Angriffe noch keine Standardprozesse der Reaktion und Bereinigung gibt. Größere Ausfälle, die für Schlagzeilen gesorgt haben (Ausfälle bei Versorgungsunternehmen, Cyberangriffe auf Hotels etc.), sind warnende Beispiele dafür, dass es keineswegs leicht ist, die Systeme wieder online zu bekommen.

ITOps und Engineering: Unter den wichtigsten Ursachen für Ausfallzeiten sind außerdem Softwarefehler ganz vorne mit dabei – was kaum erstaunlich ist: Die modernen Verfahren von Entwicklung und Bereitstellung sind komplexer und eröffnen zusätzliche Fehlerquellen. Bei 49 % der Befragten sind Softwarefehler „oft“ oder „sehr oft“ schuld an Ausfällen, bei 34 % sind es Hardwarefehler.

Die Behebung eines Softwarefehlers dauert der Befragung zufolge im Durchschnitt 16 Stunden – unserer Erfahrung nach können Unternehmen ihre Services in der Regel aber viel schneller wiederherstellen. Wir vermuten daher, dass die Befragten auch die Bereinigung der grundlegenden Ursache und die Post-Mortem-Analysen im Nachgang bei ihren Angaben berücksichtigt haben.

Die häufigsten Ausfallursachen

1. Menschliches Versagen (Cybersecurity)
2. Menschliches Versagen (ITOps)[4]
3. Software-Panne
4. Malware-Angriff
5. Hardware-Panne
6. Phishing-Angriff
7. Ausfall von Drittanbieter-Software

4 Fehlkonfigurationen der Infrastruktur, Kapazitätsprobleme und Code-Fehler in Anwendungen.

Wir haben jeden Tag Ausfallzeiten, manchmal mehrmals am Tag – Latenzprobleme, Performance-Einbußen oder Services, die komplett ausfallen.

— Poonam Khemwani, Executive Director, IT and Cloud Security Architecture, JPMorgan Chase

Oft bleiben die Ausfallursachen bestehen

63 % der Befragten aus dem Bereich Technologie geben an, dass sie immer auch die Fehler-Ursache eines Ausfalls beheben. Dass ein Incident dieser Sorte noch einmal auftritt, können sie damit allerdings nicht verhindern. In komplexen hybriden Umgebungen aus Cloud-Ressourcen und älteren Legacy-Systemen ist es ohnehin eine haarige Sache, ein Problem zu isolieren. 54 % der technischen Führungskräfte geben zu, dass sie die eigentlichen Ausfallursachen manchmal ganz bewusst nicht beheben – vielleicht deshalb, weil sie die älteren Bestandssysteme nicht noch mehr in technische Schulden treiben wollen oder weil sie ohnedies vorhaben, die veraltete Anwendung, die für den Ausfall verantwortlich ist, außer Betrieb zu nehmen.

Die Fehler-Ursachen durch Post-Mortem-Analysen aufzuspüren und zu beheben, gehört zu den Best Practices der Branche. Doch ohne die richtigen Tools wird das eine komplizierte und langwierige Aufgabe. Ordentlich durchgeführte Post-Mortem-Analysen machen die gesamte Infrastruktur robuster und zuverlässiger. Allerdings geben nur 42 % der Führungskräfte aus dem Technologiebereich an, dass ihr Unternehmen immer eine Post-Mortem-Analyse durchführt. Manchmal sind Ausfälle so schnell vorbei oder haben so geringe Auswirkungen, dass sich für viele Großunternehmen eine Untersuchung gar nicht lohnt.

Wir haben immer einen Vorteil davon, wenn wir die Fehler-Ursache finden, weil wir dann verhindern können, dass es wieder passiert. Tatsächlich wird die Downtime bei uns bis auf CEO-Ebene kontrolliert.

— Vice President of IT Architecture and Cybersecurity eines großen US-Telekommunikationsanbieters

Kluge Technologie-investitionen helfen gegen Ausfälle

„Es geht darum, die Geschäfts- und Finanzwelt darüber aufzuklären, welche Folgen es hat, wenn sie technologische Neuerungen vernachlässigt und nicht in bessere Technologien auf der Höhe der Zeit investiert.“

— Mauli Tikkiwal, IT Director und Vorstandsmitglied eines multinationalen Fertigungsunternehmens

Investitionen in Resilienz zahlen sich aus

Natürlich sind die Unternehmen bestrebt, Ausfallkatastrophen zu vermeiden, und sie tun viel dafür. Neben der Investition in Spitzenkräfte, die ihre Services am Laufen halten, geben sie im Durchschnitt pro Jahr $ 43,3 Millionen für Cybersicherheitstools ($ 23,8 Millionen) und Observability-Tools ($ 19,5 Millionen) aus.

Trotz der umfangreichen Investitionen in Prävention sichern sich Unternehmen auch gegen den Ernstfall ab. Die CFOs zahlen im Durchschnitt pro Jahr $ 34,8 Millionen für Cyberversicherungen und legen $ 13,4 Millionen für Zahlungen bei Ransomware und Cyber-Erpressung zurück. Dieser Betrag reicht in Wirklichkeit aber nicht ganz aus, denn tatsächlich überweisen die Unternehmen erpresste Summen in Höhe von $ 19 Millionen pro Jahr. Realistischerweise müssten die CFOs diese Budgets also noch aufstocken.

Lohnen sich diese Ausgaben? Den Befragten zufolge ja. Die große Mehrheit der technischen Führungskräfte gibt an, dass ihre Tools für Cybersicherheit und Observability „hilfreich“ oder „äußerst hilfreich“ gegen Ausfallzeiten sind. Die CFOs pflichten bei: Mindestens 84 % geben an, dass sie von ihren Investitionen in Sicherheit, ITOps und Engineering einen handfesten ROI zurückbekommen.

Im Bewusstsein dessen, dass Ausfallzeiten sowohl durch Cyberangriffe als auch durch Probleme bei Infrastrukturen und Anwendungen entstehen, sollten Unternehmen ihre Investitionen ebenso umfassend betrachten und Lösungen vorziehen, die beiderlei Ursachen angehen können. Für die große Mehrheit der CFOs ist der Schutz vor jederlei Ausfällen „wichtig“ oder „sehr wichtig“ in der Finanzierungsstrategie des Unternehmens.

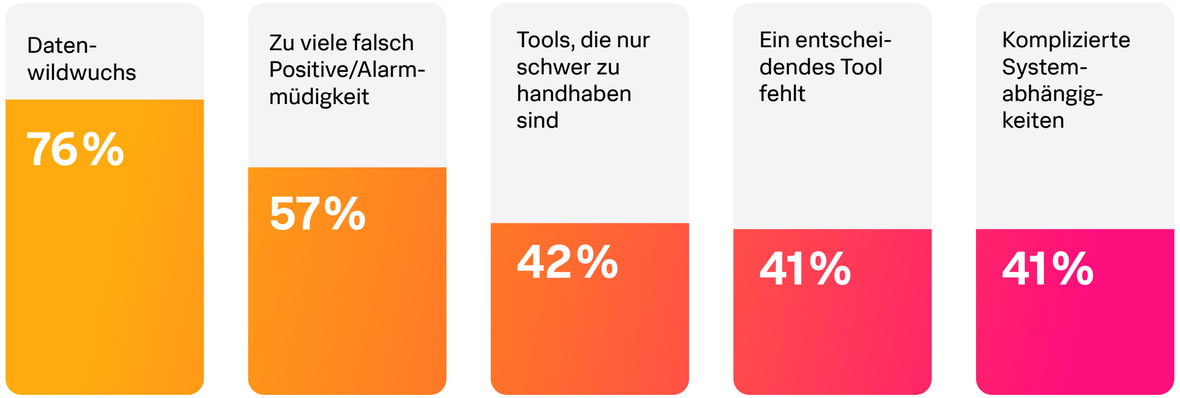
Trotz erheblicher Tool-Investitionen bleiben Ausfallzeiten eine gewaltige Herausforderung.

Explosionsartig zunehmende Datenmengen, die außerdem dezentral auf einzelne Tools und Clouds verteilt sind, sind nur schwer überschaubar. Und ohne Zugang zu den richtigen Daten zur rechten Zeit müssen die SecOps-Teams eine größere Angriffsfläche teilweise im Blindflug patrouillieren, während ITOps- und Engineering-Teams Schwierigkeiten haben, kritische Probleme zu verhindern.

„Das rasante Tempo der digitalen Transformation hat dazu geführt, dass viele Unternehmen in ihren hybriden Multicloud-Architekturen mit isolierten Tools arbeiten. Die Betriebs- und die Entwicklungsteams sitzen auf Inseln im Datenstrom fest und wissen nicht, was flussaufwärts und flussabwärts geschieht. Die technischen Schulden dieser Silo-Tools liegen darin, dass die SecOps- und die ITOps-Teams kaum Kontext bekommen und ihnen der Einblick verwehrt ist, den sie brauchen, um die erfolgskritischen Kundenanwendungen sicher am Laufen zu halten.“

— Cory Minton, Field CTO, Splunk

Die größten Probleme von Technologieverantwortlichen beim Umgang mit Ausfallzeiten



Neue Technologien sind Wagnis und Vorsprung zugleich

43 % der Befragten aus dem Bereich Technologie gestehen ein, dass ihr Entwicklungsteam sich des Öfteren außerhalb des genehmigten Stacks bewegt, um neue Technologien zu implementieren (z. B. als Schatten-IT), was zu mehr Ausfallzeiten und zu ernsten Sicherheitsvorfällen führen kann.

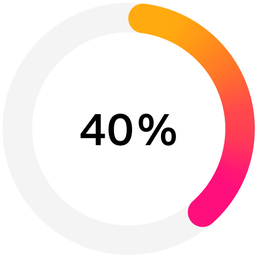
Unternehmen im Wettbewerb müssen das Eisen schmieden, so lange es heiß ist. Von daher ist es kein Wunder, dass 78 % der technischen Führungskräfte sagen, dass ihr Unternehmen das Risiko von Ausfallzeiten in Kauf nimmt, wenn es neue Technologien einführt. Das müsste aber nicht sein. In stark regulierten Branchen sind geplante Ausfallzeiten gang und gäbe. Finanzdienstleister z. B. halten branchenweit standardmäßig eine Verfügbarkeit von 99,9 % aufrecht und fahren ihre Systeme kontrolliert herunter, um neue Funktionen zu implementieren – aber außerhalb der Geschäftszeiten, sodass die Kundschaft möglichst wenig davon mitbekommt.

KI-Funktionen können Ausfallzeiten reduzieren

Den Führungskräften aus Security, IT Operations und Engineering zufolge sind im Durchschnitt sechs Tools zum Aufspüren und Beheben der Fehler-Ursachen im Einsatz. Die Palette ist breit gefächert und umfasst das Monitoring von Anwendungen, Cloud-Sicherheit, Netzwerken, Datenbanken etc. Etwa zwei Drittel der technischen Führungskräfte bezeichnen alle in unserer Befragung genannten Tools als „hilfreich“ oder „äußerst hilfreich“.

Doch keine andere Technologie hat in letzter Zeit für so viel Aufsehen gesorgt wie generative KI: 65 % nutzen derartige KI-Tools, um Ausfallzeiten zu vermeiden. 74 % davon geben an, dass sie einen erheblichen Nutzen darin erblicken. Ein Hauptgrund dürfte sein, dass diese KI-Tools auch kleinere Teams mit den Informationen versorgen, die sie benötigen, um Ausfallzeiten zu minimieren und die Systeme schnell wieder online zu bringen. Der Einsatz solcher Tools sollte jedoch immer gemäß den Corporate-Governance-Richtlinien des Unternehmens erfolgen, damit nicht ungewollt geistiges Eigentum preisgegeben wird.

Geschwindigkeit vs. Sicherheit



der CMOs finden, dass eine rasche Markteinführung wichtiger ist als Sicherheit und Zuverlässigkeit

Komplexe Anwendungsinfrastrukturen und -architekturen in Kombination mit dem dringenden Bedürfnis, Innovationen schnell an die Kundschaft zu bringen, ergeben zusammen einen perfekten Sturm menschlicher Fehler.

— Mala Pillutla, GVP of Observability, Splunk

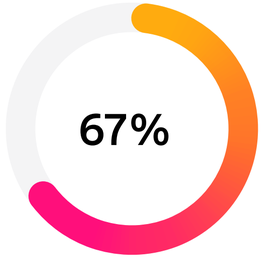
„Unternehmen investieren stark in generative KI, aber die Bedrohungsakteure sind ebenso motiviert.“

— Poonam Khemwani, Executive Director, IT and Cloud Security Architecture, JPMorgan Chase

Um die Ausfallzeiten gering zu halten, nutzt inzwischen mehr als die Hälfte der Befragten aus dem Bereich Technologie Funktionen generativer KI, die in vorhandene Tools eingebettet sind. 64 % der Befragten geben an, dass sie bereits erhebliche Vorteile daraus ziehen. Einige der nützlichsten Funktionen generativer KI sind offenbar domänenspezifische Chats (KI-Assistenten), die beim Schreiben von Abfragen und bei der Fehlersuche helfen.

Laut Lagebericht Security 2024 von Splunk sind sowohl Führungskräfte als auch Security-Fachleute optimistisch, was den Einsatz generativer KI für Use Cases der Cybersicherheit angeht, etwa zur Identifizierung von Risiken oder zur Bedrohungserkennung und Priorisierung – damit ließen sich die Security-bedingten Ausfallzeiten drastisch reduzieren. Wir sind gespannt, wie sich das in Zukunft entwickeln wird.

Generative KI wird Ausfallzeiten erhöhen



der Befragten aus dem Bereich Technologie glauben, dass die Ausfallzeiten zunehmen werden, wenn Cyberkriminelle und Bedrohungsakteure zu generativer KI greifen

Die Use Cases generativer KI zur Minimierung von Ausfallzeiten reichen von der zusammenfassenden Darstellung von Erkennungen bis zur Unterstützung bei Troubleshooting und Fehlerbehebung.

— Hao Yang, VP of Artificial Intelligence, Splunk

Die Resilienz-Leader machen es vor

„Resilienz-Leader zu sein bedeutet, nachts ruhig schlafen zu können, weil man weiß, dass das Geschäft auch dann weiterläuft, wenn das Unerwartete geschieht – und weil man weiß, dass man für Problemfälle vorgesorgt und effektive Prozesse eingerichtet hat, diese Probleme zu lösen.“

— Greg Leffler, Director of Developer Evangelism, Splunk

Resilienz-Leader sind schneller wieder da

Was zeichnet Unternehmen aus, die ihre Ausfallzeiten erfolgreich minimieren und im Ernstfall rasch wieder auf die Beine kommen? Die Mehrheit der Technologieunternehmen behauptet zwar, dass ihre Cybersicherheitsprogramme und Observability-Praktiken einen hohen Reifegrad erreicht haben, doch die Daten sprechen eine andere Sprache.

Die besten 10 % der befragten Unternehmen haben seltener Ausfallzeiten, geringere direkte Kosten und nur minimale Auswirkungen in Form von versteckten Kosten. Diese Gruppe bezeichnen wir als Resilienz-Leader.[5] Die Merkmale, die sie von anderen Unternehmen unterscheiden, ergeben eine Blaupause der Hochverfügbarkeit.

„Dass die Systemleistung nachlässt, kommt vor. Dass Systeme ganz ausfallen, gibt es eigentlich sehr, sehr selten, weil wir eine enorme Menge an Geld und Mühe in die operative Resilienz investieren, damit unsere Systeme verfügbar und einsatzfähig bleiben.“

— Chris Russell Miller, Head of IT and Cyber Risk, BNP Paribas Personal Finance UK

Die Resilienz-Leader können ihre Systeme nach Ausfällen schneller wieder zum Laufen bringen. Die Mean Time to Recover (MTTR) bei anwendungs- oder infrastrukturbedingten Ausfällen ist bei ihnen im Durchschnitt um 28 % kürzer als bei der Mehrheit der Befragten. Bei Cybersecurity-Incidents sind sie um 23 % schneller wieder auf den Beinen.

Schnellere Wiederherstellung bedeutet bessere Customer Experience, weniger unerwünschte Medienaufmerksamkeit und weniger verärgerte End-User.

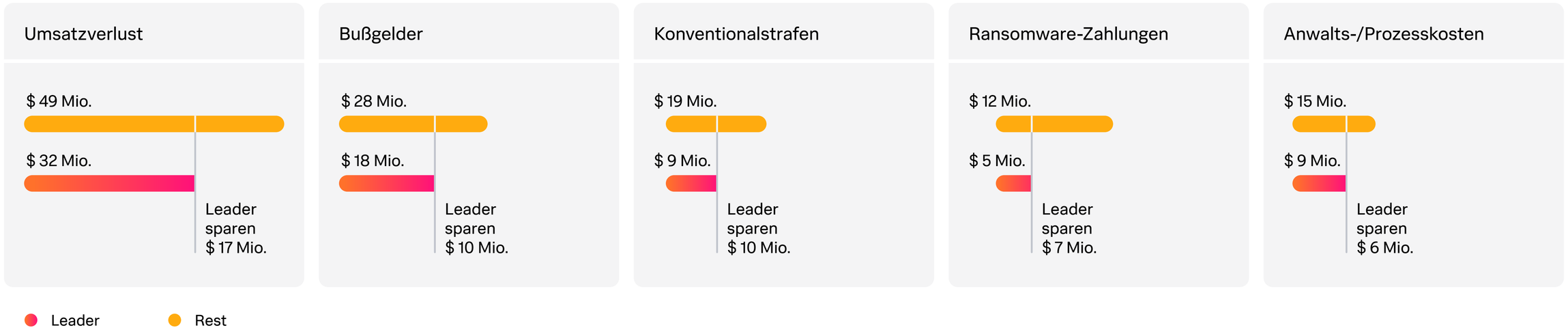
Resilienz-Leader beheben Probleme schneller als der Rest

5 Die Zugehörigkeit zur Gruppe der Resilienz-Leader errechnet sich aus der Häufigkeit von Ausfallzeiten und der Höhe des wirtschaftlichen Schadens durch versteckte Kosten..

Resilienz-Leader kommen ohne größeren Schaden davon

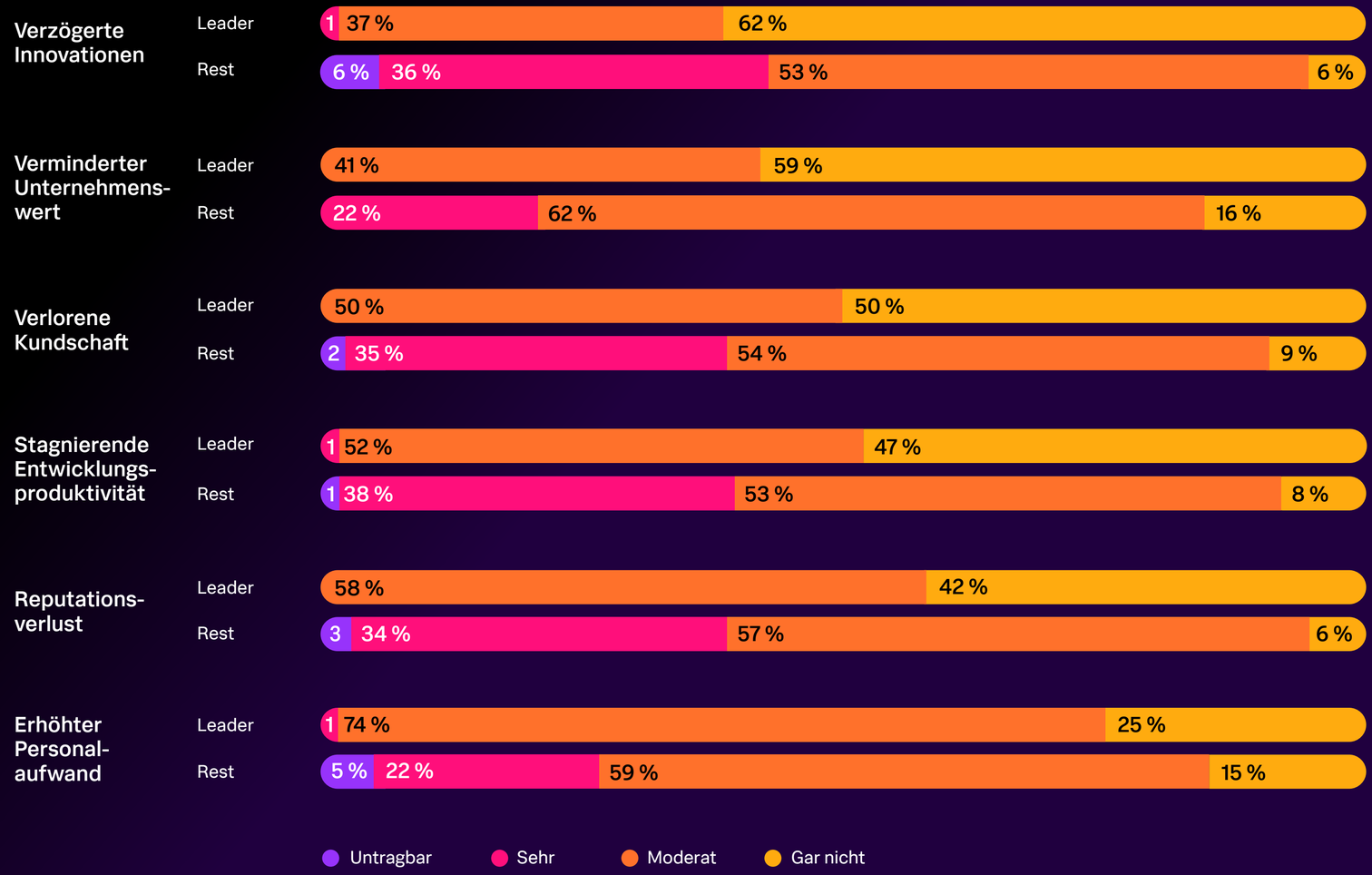
Die Leader haben 245 Stunden weniger anwendungs- oder infrastrukturbezogene Ausfälle pro Jahr als der Rest. In puncto Cybersicherheit sind die Ausfallzeiten bei ihnen 224 Stunden kürzer. Resiliente Unternehmen halten die direkten Kosten und finanziellen Verluste von Ausfallzeiten minimal und werden auch weniger empfindlich von versteckten Kosten getroffen.

Die direkten Kosten von Ausfallzeiten sind für Resilienz-Leader geringer



Die Resilienz-Leader haben weniger unter versteckten Kosten zu leiden. Kein einziger aus dieser Gruppe beschreibt den wirtschaftlichen Schaden als „untragbar“, die meisten erleiden überhaupt keinen Schaden oder stufen ihn als „moderat“ ein. Zum Vergleich: Die restlichen 90 % der Unternehmen bezeichnen die Auswirkungen versteckter Kosten als „einigermaßen“ oder „sehr“ schädlich.

Die Schäden durch versteckte Kosten von Ausfallzeiten sind für Leader geringer



Rundungsbedingt ergeben die Prozentsätze unter Umständen nicht 100 %.

Resilienz-Leader handeln vorausschauend

Resilienz-Leader haben beim Einsatz generativer KI einen höheren Reifegrad erreicht, sie nutzen eigenständige Tools mit generativer KI fünfmal häufiger in zunehmendem Umfang und Funktionen generativer KI als Integrationen in vorhandenen Tools viermal häufiger.

Die Resilienz-Leader investieren auch sonst in zukunftsorientierte Technologien. Sie geben im Durchschnitt $ 8 Millionen mehr für zusätzliche Infrastrukturkapazitäten als der Rest, $ 11 Millionen mehr für Cyberversicherungen und $ 10 Millionen mehr für Backups.

Die Resilienz-Leader investieren außerdem $ 12 Millionen mehr in Cybersicherheitstools und $ 2,4 Millionen mehr in Observability-Tools. Und das ist offenbar das Mindeste. Denn auf die Frage, ob sie ihre derzeitigen Ausgaben für solche Tools als angemessen empfinden, antworten die Leader eher mit Nein – wir vermuten daher, dass der Gruppe von Unternehmen, die mit Ausfallzeiten besonders erfolgreich umgeht, deutlicher bewusst ist, welche Auswirkungen Ausfälle auf den Geschäftsbetrieb haben können und dass Ausfallzeiten eine Herausforderung sind, die sich immer wieder neu stellt.

Angesichts all dieser Ausgaben stellt sich die Frage: Ist Resilienz schlicht eine Frage des Budgets?

Nicht unbedingt. Wir haben eher den Eindruck, dass die Resilienz-Leader zwar mehr investieren, aber vor allem klüger. Denn wo der Schwerpunkt auf Datenmanagement und Tool-Konsolidierung liegt, ergeben sich innovativere Strategien für Sicherheit und Observability. Das heißt: Geringere Investitionen führen dann zu besseren Ergebnissen wie umfassender Transparenz und übergreifender Zusammenarbeit und ermöglichen einen proaktiven Ansatz in puncto Ausfallzeiten.

Resiliente Unternehmen sind sich der finanziellen Folgen von Ausfallzeiten bewusst. Sie nehmen wahr, was sich direkt und indirekt über und unter der Oberfläche abspielt, und sie investieren gezielt, um Ausfälle und deren Folgen von vornherein zu unterbinden. Zum Glück ist die große Mehrheit der Befragten aus dem Bereich Technik der Ansicht, dass die negativen Auswirkungen von Ausfallzeiten nicht akzeptabel sind. Es geht also in die richtige Richtung.

Du kannst einem Problem den ganzen Tag lang Geld hinterherwerfen, ohne es damit zu lösen. Resilienz-Leader zu sein bedeutet, ein Mindset zu haben, das Ausfallzeiten nicht akzeptiert – und deshalb Prozesse und Praktiken zu etablieren, die das ermöglichen.

— Greg Leffler, Director of Developer Evangelism, Splunk

Resilienz-Leader sind unterwegs in eine KI-gestützte Zukunft

Einsatz generativer KI bei den Leadern

Eigenständige Tools mit generativer KI:

KI-Funktionen als Integrationen in vorhandenen Tools:

Einsatz generativer KI beim Rest

Eigenständige Tools mit generativer KI:

KI-Funktionen als Integrationen in vorhandenen Tools:

Noch nicht · Evaluation · Pilotphase · Zunehmend

Rundungsbedingt ergeben die Prozentsätze unter Umständen nicht 100 %.

So kann Ihr Unternehmen Ausfallzeiten minimieren

„Digitale Resilienz bedeutet nicht nur, Ausfallzeiten minimal zu halten. Es bedeutet, in der Welt von heute erfolgreich zu sein.“

— Mala Pillutla, GVP of Observability, Splunk

Leader-Tipps: Wie erfolgreiche Unternehmen Resilienz aufbauen

In einer resilienteren Welt werden die Unternehmen kurzfristig profitieren, das durchaus. Aber sie werden auch eine langfristig stabile Wertschöpfung erleben. Fast die Hälfte der Führungskräfte aus den Bereichen Sicherheit, IT und Engineering findet ihre Ausfallzeiten inakzeptabel. Die Unternehmen wissen, dass zu viel auf dem Spiel steht, für sie selbst und für ihre Kundschaft. Es geht um nichts weniger als darum, das Vertrauen von End-Usern, Kundschaft und Investoren zu erhalten, das gilt für Händler ebenso wie für kritische Infrastrukturen.

Doch angesichts schwankender Budgets, neuer Regulierungen und der Eigenheiten regionaler Infrastrukturen fällt es den Verantwortlichen nicht leicht, Ausfallzeiten und deren kostspielige Folgen konsequent zu vermeiden. Aufgrund der Datenlage aus der Befragung und anhand der Merkmale erfolgreicher Resilienz-Leader können wir die folgenden Empfehlungen geben.

1. Notfallplan für Ausfälle erarbeiten.

Ausfallzeiten sind unvermeidlich. Darum ist es erfolgsentscheidend, dass das Unternehmen über geeignete Prozesse und Tools verfügt. Zu den elementaren Hygienemaßnahmen gehört, dass jede Anwendung instrumentiert ist, dass ein Runbook für Ausfälle vorliegt und Schritt für Schritt befolgt wird, dass Verantwortliche auf Engineering-Seite benannt sind – und dass auch alle darüber informiert sind, wer zuständig ist. Außerdem sollten Sie mit Ihren SecOps-, ITOps- und Engineering-Teams im Rahmen regelmäßiger Tabletop-Übungen Ausfallszenarien durchspielen und damit Ihre Reaktionen bei Downtime-Events testen und trainieren. Oder Sie arbeiten direkt mit Chaos Engineering, also mit zufallsartig generierten Realfehlern, die aufzeigen, wie weit ihre Systeme solchen Events gegenüber resilient sind.

2. Post-Mortem-Analysen durchführen – und im Zweifelsfall die Voraussetzungen dafür schaffen.

Sie möchten verhindern, dass ein Problem, das zu Ausfällen geführt hat, noch einmal auftritt? Dann ist eine gründliche Fehler-Ursachen-Analyse im Verlauf des Incidents das erste Mittel der Wahl. Die Analyse kann den ursprünglichen Fehler ausfindig machen und Lösungen aufzeigen. Weil das aber nicht immer auf Anhieb klappt, sollten Sie in Observability-Tools investieren, bestehende Silos aufbrechen und die Daten aus Ihren gesamten Umgebungen zentral erfassen und überschaubar machen. Dann haben Sie Tool-unabhängig einfachen Zugang zu sämtlichen relevanten Informationen und können auch noch im Nachgang rigorose Post-Mortem-Analysen durchführen und so letztlich verhindern, dass sich solche Vorfälle wiederholen.

3. Geistiges Eigentum schützen.

Wenn Sie ein großes Sprachmodell (LLM) mit dem geistigen Eigentum des Unternehmens trainieren, sollten Sie sich der Risiken dieses Vorgehens bewusst sein. Stellen Sie also klare Data-Governance-Richtlinien auf und schützen Sie das Unternehmen vor Datenverlusten. Und denken Sie daran: Eigenständige Tools mit generativer KI sind nur der erste Schritt. Der nächste besteht in KI-Funktionen, die in Ihre bestehenden Tools integriert sind, etwa Chat-Assistenten – damit beugen Sie Ausfällen noch effektiver vor. Solche domänenspezifischen Assistenten können die Produktivität steigern und außerdem der Belegschaft zu neuen, besseren Skills verhelfen, wovon das Unternehmen auf lange Sicht profitiert.

4. Gemeinsame Datengrundlage der Zusammenarbeit für Teams und Tools schaffen.

Ausfallursachen gibt es überall. Darum ist umfassende Transparenz, die alle Bereiche von SecOps, ITOps und Engineering umfasst, absolut erfolgsentscheidend. Wenn Ihre Teams Daten, Kontext und Tools gemeinsam nutzen können, fällt ihnen die Zusammenarbeit leichter. Dann können sie im Ernstfall Probleme schneller beheben, Fehler-Ursachen schneller identifizieren und den Betrieb eher wieder aufnehmen.

5. Proaktiv gegen Ausfallzeiten vorgehen und verhindern, dass Probleme eskalieren.

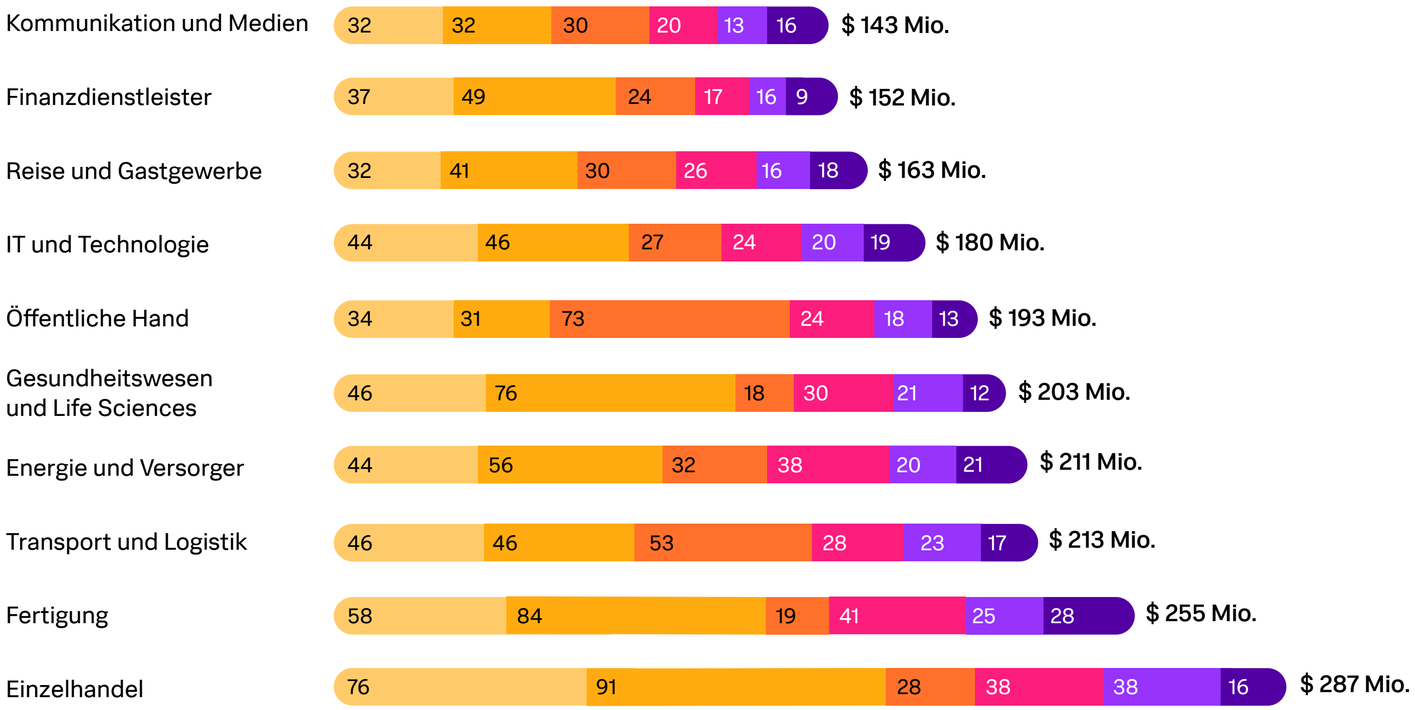
Erfolg versprechen Investition in KI- und ML-gestützte Lösungen zur Mustererkennung und ein proaktives Programm zur Vermeidung von Ausfallzeiten, das auf die Zusammenarbeit der SecOps-, ITOps- und Engineering-Teams ausgelegt ist. Durch KI-gestützte vorausschauende Analysen können Sie Ihre SOC-Kapazitäten vervielfachen und verhindern, dass sich Probleme zu Katastrophen auswachsen.

Ausfallzeiten wirken sich je nach Branche anders aus

Die Downtime ist zwar in jeder Branche in etwa gleich, doch die Kosten dieser Ausfallzeiten variieren beträchtlich.

Es liegt auf der Hand, dass Ausfallzeiten den Einzelhandel empfindlicher treffen als alle anderen Branchen. Weniger offensichtlich ist die Abhängigkeit der Branchen voneinander: Wenn Finanzdienstleister ausfallen, ist praktisch alles andere auch betroffen – Ausfälle in dieser Branche ziehen automatisch Ausfallzeiten in anderen Branchen nach sich. Ausfälle in der Herstellung wiederum wirken sich auf die gesamte Lieferkette und auf die nachgelagerten Unternehmen der Logistik und des Handels aus. Ausfälle bei Kommunikation und Medien legen den Finanzsektor und abermals den Einzelhandel lahm. Am meisten beunruhigend ist jedoch, dass Ausfälle bei Kommunikation und Medien die Bevölkerung von Notfalldiensten abschneiden und eine koordinierte Reaktion im Katastrophenfall unmöglich machen.

Die Kosten von Ausfallzeiten summieren sich in jeder Branche



Aufschlüsselung der Kostenkategorien (in $ Mio.):

Umsatzverlust	
Recht/Verträge	Bußgelder, Konventionalstrafen, Anwalts-/Prozesskosten
Schadensbegrenzung	Markenkampagnen, PR/Investor Relations
Sicherheit	Ransomware-Zahlungen, Cyberversicherungsprämien, erpresste Gelder
Produktivität	Lohnkosten für Überstunden, Produktivitätsverluste
Technik	Zusätzliche Infrastrukturkapazitäten, Wiederherstellung aus Backups

Kostenvergleich nach Weltregion

Aufgrund von Faktoren wie den rechtlichen Rahmenbedingungen und der digitalen Infrastruktur spielt der geografische Standort bei den Downtime-Kosten eine Rolle. 89 % der Befragten aus dem Bereich Technologie geben an, dass die Ausfallzeiten von der Qualität der digitalen Infrastruktur vor Ort abhängen.

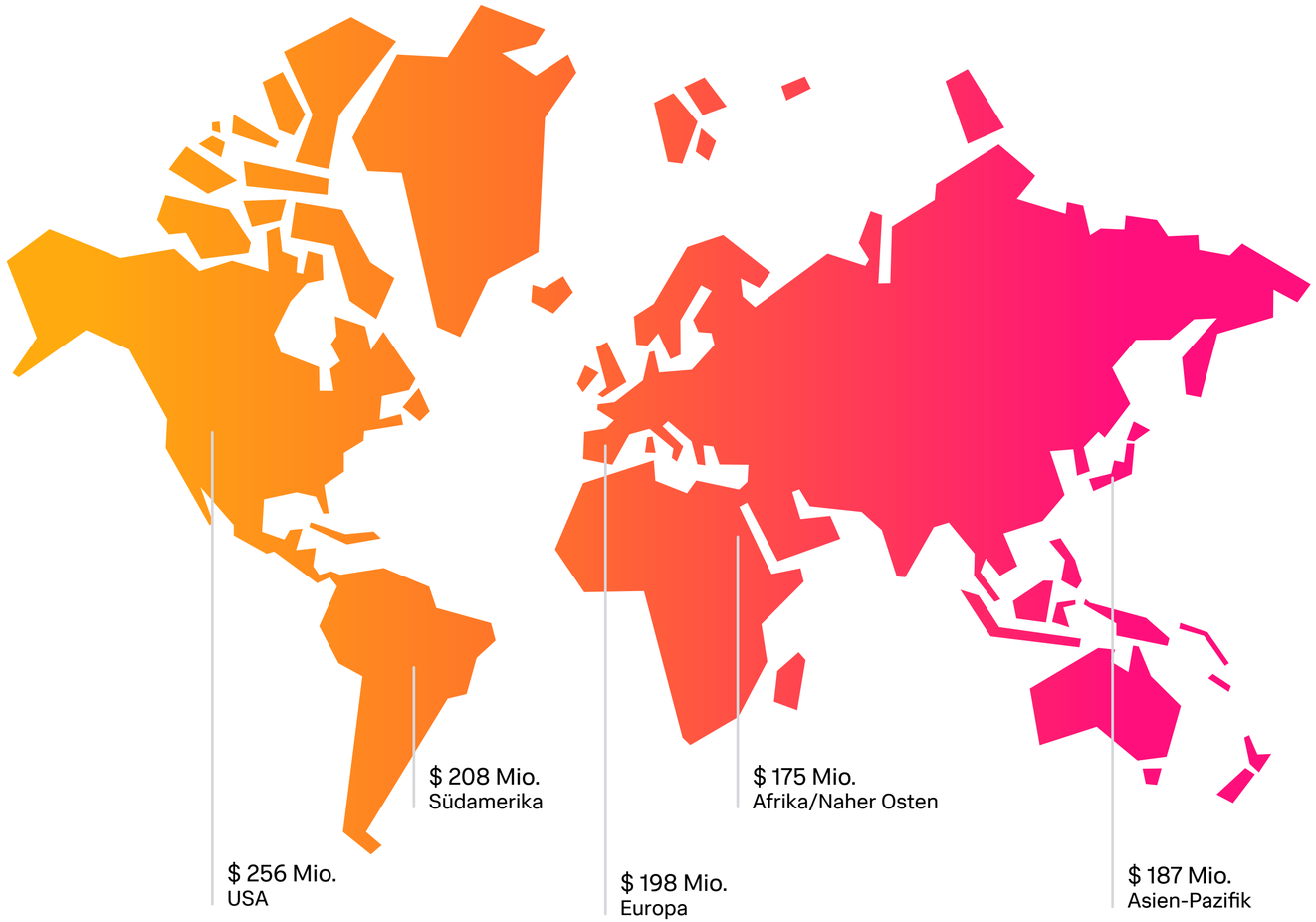
Ausfallzeiten kommen US-Unternehmen im weltweiten Vergleich am teuersten zu stehen, vor allem aufgrund von direkten Umsatzverlusten ($ 68 Millionen) und Konventionalstrafen ($ 27 Millionen). US-Unternehmen haben auch höhere Anwalts- und Prozesskosten ($ 19 Millionen) und zahlen höhere Cyberversicherungsprämien ($ 14 Millionen). Auch sind die Ausgaben für zusätzliches Marketing ($ 31 Millionen) in den USA höher.

Die Kosten in Gestalt von Geldbußen ($ 29 Millionen) und Produktivitätsrückgang ($ 11 Millionen) sind bei den Unternehmen in Europa genauso hoch wie in den USA. Allerdings zahlt Europa mehr für Überstunden ($ 12 Millionen) und für die Wiederherstellung aus Backups ($ 9 Millionen).

Afrika und der Nahe Osten haben zwar die niedrigsten Gesamtkosten, sie zahlen aber am meisten für Ransomware ($ 22 Millionen) und Cyber-Erpressung ($ 12 Millionen).

Die geografische Lage hat auch Einfluss darauf, wie schnell sich die Marke, der Erlös und der Aktienkurs nach einem Incident und dessen Behebung wieder erholen. Europa und die asiatisch-pazifische Region brauchen am längsten, während die Unternehmen in Afrika und im Nahen Osten in allen drei Kategorien am schnellsten zur Normalität zurückkehren.

In den USA schlagen Ausfallzeiten deutlich heftiger zu Buche als anderswo



Sorgen Sie mit Splunk für digitale Resilienz

Podcast Digitaler Kompass: Unternehmen auf Kurs Richtung digitale Resilienz

Neugierig auf weitere hilfreiche Erkenntnisse zu aktuellen Tech-Trends und darüber hinaus? Erfahren Sie, wie Leader die drängendsten Cyber-Herausforderungen von heute angehen: KI, neue Bedrohungen, Compliance-Vorgaben und mehr.

Mehr erfahren

Im Wettlauf um KI-Vorteile

Auf dem Weg Richtung digitale Resilienz begegnen Security-Verantwortliche vielen Herausforderungen, allen voran künstlicher Intelligenz. Erfahren Sie, wie Ihr Unternehmen KI zum eigenen Vorteil nutzen und sich gegen die Gefahren von KI wappnen kann.

Bericht lesen

Methodik

Oxford Economics hat für diese Studie eine Hybrid-Umfrage mittels CATI- (Computer-assisted Telephone Interviewing) und Online-Methoden durchgeführt und dabei 2.000 Führungskräfte der Global-2000-Unternehmen befragt. Erfasst wurden Unternehmen aus 53 Ländern (Afrika, Asien-Pazifik, Europa, Naher Osten, Nordamerika und Südamerika) und zehn Branchen (Energie und Versorgung, Finanzdienstleister, Gesundheitswesen und Life Sciences, IT und Technologie, Fertigung, Kommunikation und Medien, öffentliche Hand, Einzelhandel, Transport und Logistik sowie Reise und Gastgewerbe). Tätig sind die Befragten in den Bereichen Technologie (einschließlich Sicherheit, IT und Engineering), Finanzen (einschließlich Chief Financial Officers) und Marketing (einschließlich Chief Marketing Officers).

Wie Oxford Economics die Kosten von Ausfallzeiten kalkuliert

Die Kosten der Ausfallzeiten für die Global 2000 wurden von Oxford Economics durch Abbildung der Befragungsantworten auf die 2023er Werte der Global 2000 ermittelt. Anhand der Antworten wurden die Downtime-Kosten in Relation zum Gewinn gesetzt (als Prozentwert, um Unterschiede in der Unternehmensgröße auszugleichen). Die typischen Kosten pro Erlöseinheit wurden dann durch Abgleich des länderspezifischen Medians der vorigen Kennzahl mit den Umsatzdaten jedes Unternehmens der Global 2000 im Finanzjahr 2023 kalkuliert. Durch diese Art und Weise der Skalierung lassen sich die Antworten der Befragung mit Rücksicht auf die Größen und die regionale Verteilung der Global-2000-Unternehmen normalisieren und vergleichbar machen.

Über Splunk

Splunk, ein Unternehmen von Cisco, macht Organisationen digital resilienter. Führende Unternehmen nutzen unsere Plattform für einheitliche Security und Observability, um ihre digitalen Systeme sicher und zuverlässig zu halten. Unternehmen vertrauen auf Splunk, um zu verhindern, dass sich Sicherheits-, Infrastruktur- und Anwendungsprobleme zu größeren Vorfällen entwickeln, um Beeinträchtigungen durch digitale Störungen zu reduzieren, und um neue Chancen zu erkennen und zu ergreifen.

Bleiben Sie dran und reden Sie mit:

splunk>

24.CMP.report.the-hidden-costs-of-downtime_v13_GER