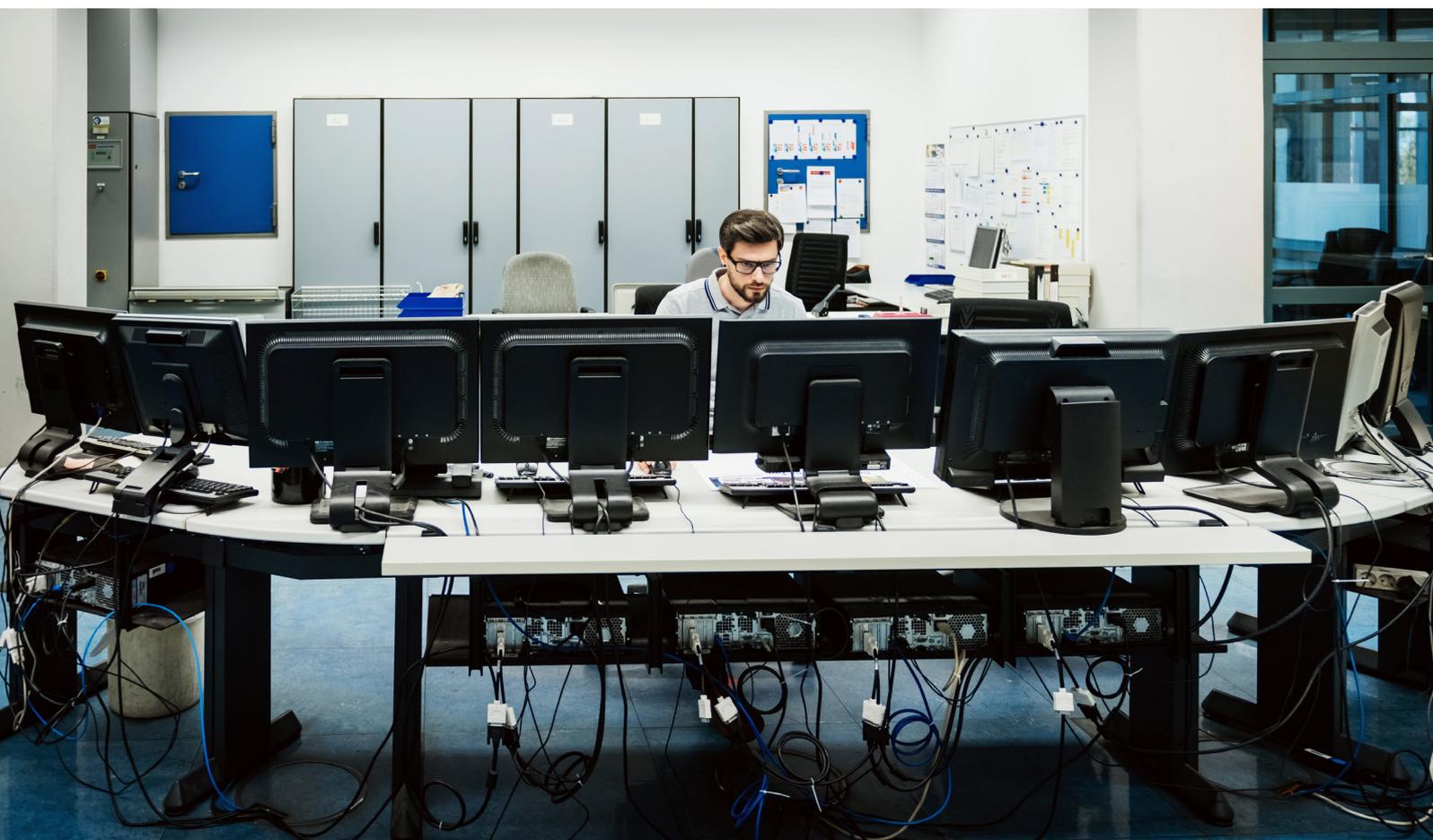


Die Stunde der CIOs in der ersten Phase der Corona-Krise

Von Aamer Baig, Klemens Hjartar und Steve Van Kuiken



„Alle Augen sind auf mich gerichtet. Und ich kämpfe mit einer Explosion des Online-Datenvolumens, der Remote- Zugriffe durch Mitarbeiter im Home Office und mit neuen Cyberbedrohungen. Jeden Tag ist etwas anderes.“

Aus diesem Zitat des Chief Information Officers (CIO)

einer Bank spricht der Druck, unter dem die Technologieverantwortlichen momentan stehen. CIOs sehen sich mit der größten Herausforderung ihrer Karriere konfrontiert: IT-Infrastrukturen gehen in die Knie, Denial-of-Service-Angriffe legen Server lahm und Websites brechen unter zu vielen Zugriffen zusammen. Während die Unternehmen mit den [Auswirkungen der Covid-19-Pandemie](#) kämpfen, ist bereits klar, dass CIOs für das Überwinden der Krise eine zentrale Rolle spielen.

Die Covid-19-Pandemie ist zuallererst eine menschliche Tragödie, bei der die Technologie an vorderster Front steht. Viele der beruflichen und privaten Veränderungen – von der Arbeit im Home Office bis hin zur Verlagerung der Einkäufe ins Internet – stützen sich darauf. Und da die Technologie so viele Aspekte eines Unternehmens miteinander verbindet, wissen CIOs wie niemand sonst, was tatsächlich geschieht und wie sich die Situation meistern lässt.

Covid-19 ist ein globales Phänomen, wobei sich Unternehmen von Asien über Europa bis nach Nord- und Südamerika bei der Reaktion auf die Krise in unterschiedlichen Phasen befinden. Wir können beobachten, dass es im Wesentlichen drei Wellen gibt: In der ersten gilt es, Stabilität zu gewährleisten, den Geschäftsbetrieb aufrechtzuerhalten und gleichzeitig die Krise einzudämmen. In der zweiten Welle etablieren die Unternehmen neue Arbeitsweisen. In der dritten Welle heißt es, Lektionen aus der Krise zu ziehen und eine technologische Transformation zu konzipieren, die Unternehmen für ähnliche Situationen in der Zukunft resilienter macht.

Dieser Artikel konzentriert sich darauf, wie CIOs die erste Welle meistern können und wie es ihnen gelingt, nicht mehr nur zu reagieren, sondern der Entwicklung

irgendwann einen Schritt voraus zu sein. CIOs, die ihre Unternehmen erfolgreich durch die erste Welle der Krise leiten, können unserer Überzeugung nach nicht nur das Kerngeschäft stabilisieren, sondern sich auch einen Ruf als effektive Führungskräfte sichern.

Wir haben in den vergangenen Monaten mit mehr als 100 CIOs von globalen Unternehmen gesprochen. Diese Diskussionen und unsere Erfahrungen aus früheren Wirtschaftskrisen sprechen dafür, dass CIOs in den nächsten 60 bis 90 Tagen ihre Energie auf die folgenden zehn Maßnahmen fokussieren sollten:

Auf das konzentrieren, was jetzt wichtig ist

1. Sich um die Mitarbeiter kümmern. Covid-19 ist eine menschliche Tragödie. Oberste Priorität muss es für CIOs deshalb haben, sich um die Beschäftigten und deren Familien zu kümmern. Es ist wichtig zu erkennen, dass sich die Menschen jetzt zunächst um ihre Familien sorgen, ihre Kinder betreuen, die nicht mehr zur Schule gehen können, Vorräte aufstocken und sich bemühen, gesund zu bleiben. Nebenbei versuchen sie noch, ihre Arbeit zu erledigen. Dies erfordert von CIOs Empathie und Flexibilität.

CIOs bieten jetzt flexible Arbeitsmodelle mit Remote-Arbeitsplätzen, verschiedenen Schichten und Lösungen für Personalausfälle. Ein CIO hat erkannt, dass sich die Schließung der Schulen auf die Mitarbeiter im Home Office auswirkt, und schnell für jeden unentbehrlichen Beschäftigten ein Backup-Support-Modell konzipiert. Amazon USA hat zugesagt, Mitarbeitern, die an Covid-19 erkranken, ihr Gehalt weiterzuzahlen, damit sie sich die Zeit nehmen können, gesund zu werden, ohne sich wegen Einkommensausfällen Sorgen zu machen.¹

¹ Jonathan Schieber: „Establishing an emergency-relief fund, Amazon commits to two week pay for workers affected by COVID-19“, TechCrunch, 11. März 2020, techcrunch.com.

Denjenigen, die weiterhin ins Unternehmen kommen, müssen CIOs ein sichereres Arbeitsumfeld bieten. Eine Firma hat sechs Arbeitszonen eingerichtet, zwischen denen die Mitarbeiter nicht hin- und herwechseln können. Wenn jemand erkrankt, wird die betreffende Zone schnell isoliert. Ein europäisches Finanzinstitut lässt das Management in Schichten arbeiten, damit die wichtigsten Führungskräfte nicht im selben Raum sind; außerdem gibt es Backups für Topmanager und Mitarbeiter in unverzichtbaren Führungspositionen.

Diese Fokussierung auf das Personal erstreckt sich auch auf die Kooperation mit Zeitarbeitskräften und externen Dienstleistern, von denen viele im Unternehmen vor Ort arbeiten. Der CIO einer anderen Bank hat alle externen Dienstleister kontaktiert und gefragt, wo sie sich in den vergangenen zwei Wochen aufgehalten haben und welche Pläne sie für die nächste Woche haben. So konnte er besser klären, wer wirklich vor Ort sein musste und wer nicht, um das Risiko für seine eigenen Angestellten zu senken.

Wie erfolgreich ein CIO dabei ist, den Beschäftigten in dieser Krise beizustehen, dürfte sich erheblich auf die künftige Loyalität und Mitarbeiterbindung auswirken.

2. Souverän, einheitlich und verbindlich kommunizieren. Unsicherheit stiftet Angst und Verwirrung. Dem müssen CIOs mit einem Krisenkommunikationsprogramm entgegenwirken, das sowohl dem Topmanagement als auch den Angestellten klar sagt, wie die Lage aussieht und welche Maßnahmen ergriffen werden. Regelmäßige Briefings sorgen für eine gewisse Routine – das schafft Vertrauen. Verzögerungen größerer Einsätze müssen geplant und kommuniziert werden.

Das „Wie“ kann ebenso entscheidend sein wie das „Was“. Ein CIO schickt der gesamten Belegschaft regelmäßige SMS-Updates, weil er der Meinung ist, es sei wichtiger, dass die Kommunikation menschlich ist, als dass sie aus offiziellen Unternehmenskanälen kommt.

Zuhören und Lernen sind ebenfalls entscheidend. Die Lage ändert sich so schnell, dass der CIO der oberste „Lernende“ sein muss, um der gesamten Organisation zu helfen, mit den voranschreitenden Veränderungen immer besser umzugehen. Einfach nur Technologie bereitstellen reicht nicht. CIOs müssen sich an unterschiedliche Stakeholder wenden und ein besseres Verständnis für ihre Bedürfnisse entwickeln, um die richtigen Lösungen anbieten zu können. Darüber hinaus sollten CIOs die Beschäftigten an Remote-Arbeitsplätzen fragen, was funktioniert und was nicht; so können sie die Fähigkeiten und Supportniveaus optimieren.

3. Jenseits von Technologie das Home-Office-Modell zum Erfolg führen. Dass jetzt plötzlich viel mehr Mitarbeiter von zu Hause arbeiten – in einem europäischen Unternehmen ist die Zahl der Remote-Arbeiter buchstäblich über Nacht um das 15 Fache gestiegen – bringt eine Vielzahl von Problemen mit sich: von unzureichenden Videokonferenzmöglichkeiten bis hin zu schlechten Internetverbindungen bei den Angestellten zu Hause. CIOs müssen hier zügig den CEO beraten und dem Unternehmen zeigen, wie Remote-Arbeitsmodelle am besten funktionieren, bevor sich jede einzelne Abteilung ihre eigenen Kollaborationstools aussucht. Viele CIOs kaufen bereits zusätzliche Lizenzen und erweitern ihre Netzwerkkapazitäten, um mehr Zugriffe zu ermöglichen. Bei Problemen mit langsamen Internetverbindungen bei den Mitarbeitern zu Hause können CIOs Abhilfe schaffen, indem sie 4G-/5G-Modems bereitstellen oder die Kosten für leistungsstärkere Internettarife und Datenpakete erstatten.

Die Technologie ist aber letztlich nur ein Werkzeug. Wenn neue Arbeitsweisen funktionieren sollen, braucht es einen Kulturwandel. Hier können CIOs mit Best Practices und wirksamen Lerneinheiten helfen. Sie können Tests vorantreiben, aus unterschiedlichen Ansätzen lernen und die Erkenntnisse ans Unternehmen zurückmelden. Krisenmanagement ist eine funktionsübergreifende Disziplin, und der CIO ist prädestiniert dafür, die neuen Arbeitsweisen zu ermöglichen.

4. Neue Arbeitsweisen vorantreiben. Wenn die Mitarbeiter ihr Arbeitsverhalten umstellen, sehen sich viele einer Fülle von Tools gegenüber, die sie oft nicht effektiv einzusetzen wissen. Ein CIO sagt: „Die Verbreitung von neuen Tools und Protokollen zu gewährleisten ist bislang der frustrierendste Teil des ganzen Prozesses.“

Bis sich neue Verhaltensweisen durchsetzen, dauert es in der Regel rund 30 Tage; deshalb müssen CIOs in den nächsten vier Wochen aggressiv dafür werben. Als Faustregel gilt: Die Beschäftigten dazu zu bringen, ein neues Tool einzusetzen, erfordert ungefähr den doppelten Investitionsaufwand wie die eigentliche Entwicklung des Tools. Klare Anleitungen für Tools und Verfahren (zum Beispiel für das Herunterladen notwendiger Apps oder den Einsatz von Multifaktorauthentifizierung) sind notwendig. Allerdings ist es noch viel wichtiger, in Nudging-Techniken, gute Schulungen und Zertifizierungen zu investieren, um dafür zu sorgen, dass neue Tools nicht nur eingeführt werden, sondern den Mitarbeitern auch tatsächlich bei ihrer täglichen Arbeit helfen.

Vorbilder sind ebenfalls essenziell, um Verhaltensweisen zu beeinflussen, etwa das Kommunizieren über Kollaborationstools, Meetings per Zoom, Skype oder WebEx und das Aktivieren der Kamera am Rechner. Der CEO eines großen Pharmakonzerns hat bei Videokonferenzen explizit vorgeschrieben, dass alle ihre Kameras „einschalten“.

5. Proaktiv für mehr Sicherheit sorgen. Angreifer versuchen mit Cyberattacken verstärkt, die aktuelle Verwirrung und Unsicherheit auszunutzen. Einige geben sich in E-Mail-Phishing-Kampagnen als Mitarbeiter des Helpdesks aus und bitten Beschäftigte, ihre Zugangsdaten per SMS zu bestätigen (diese Kombination aus SMS und Phishing ist auch als Smishing bekannt). Remote Working schafft zusätzliche Risiken: Manche Angestellten versuchen, Sicherheitskontrollen zu umgehen, um ihre Aufgaben von zu Hause aus erledigen zu können. Die Nutzung von VPN-Zugängen (VPN: Virtual Private Network) in nie gekanntem Ausmaß erschwert die Sicherheitsüberwachung von Netzwerken; außerdem kann das Remote Working Abschreckungsmaßnahmen gegen Bedrohungen im Unternehmen einschränken.

Als Reaktion darauf müssen sich CIOs in enger Zusammenarbeit mit ihren obersten IT-Security-Verantwortlichen auf das Thema Sicherheit konzentrieren. Das bedeutet insbesondere, Remote-Zugänge zu sensiblen Daten oder Software-Entwicklungsumgebungen sicherer zu machen und Multifaktorauthentifizierungen für Remote-Arbeiter einzuführen. Darüber hinaus müssen Unternehmen die Aufmerksamkeit ihrer Beschäftigten auf sichere Remote-Working-Abläufe, das Erkennen von Bedrohungen und Eskalationsabläufe lenken. Notfallpläne (zum Beispiel für Disaster Recovery, Nachfolgepläne für externe Dienstleister, Backups für Technologierisiken) sind sofort zu testen. Unternehmen, die keine solchen Notfallpläne haben, müssen diese erstellen und prüfen. Es ist außerdem notwendig, dass CIOs mehr Ressourcen für die Überwachung bereitstellen (zum Beispiel für die Netzwerkverfügbarkeit, neue Malware-Varianten und Endpoint-Datenzugänge), um die Reaktionszeiten im Risikofall zu verkürzen.

Kernsysteme und Geschäftsbetrieb stabilisieren

6. Kritische Infrastruktur, Systeme und Prozesse stabilisieren. Massive Veränderungen in den Arbeitsabläufen und Verhaltensweisen von Mitarbeitern und Kunden stellen in jedem Unternehmen eine nie gekannte Belastung für die Infrastruktur dar. Internetanbieter verzeichnen in stark betroffenen Ballungsräumen eine Verschlechterung der Verbindungsqualität, weil die Leitungen und Netzwerke durch Remote-Arbeiter überlastet sind.

Auch die Lieferzeiten für Infrastrukturkomponenten sind aufgrund von Störungen in den asiatischen Lieferketten deutlich länger als üblich, zum Beispiel für Server, Speicher, Ersatzteile und Netzwerkzubehör.

Das fieberhafte Bestreben, möglichst schnell zu handeln, birgt die Gefahr, nur noch blind jedem neuen Notfall hinterherzuhetzen. CIOs sollten einen Schritt zurücktreten und sich einen Überblick darüber verschaffen, welche Systeme und Anwendungen am wichtigsten sind, und deren Stabilisierung priorisieren. Dazu gehört eine Szenarioplanung, um sich auf kommende Probleme vorzubereiten. Sie sollten sich zum Beispiel einen Vorrat an notwendigen Ersatzteilen und Hardware (wie PCs oder iPhones) anlegen und einen Bereitstellungsprozess konzipieren, um diese Dinge dorthin zu bringen, wo sie gebraucht werden. Außerdem müssen CIOs neben den dringlichsten Aufgaben (wie das schnelle Aufstocken der Infrastrukturkapazität, der Netzwerkbandbreite und der VPN-Zugänge) auch die Auswirkungen durchdenken, die ein oder zwei Schritte später zu erwarten sind.

Es müssen eine Reihe von Szenarien entwickelt und getestet werden, einschließlich extremer Anwendungsfälle. Ein CIO hat Infrastruktur und Netzwerk einer Prüfung unterworfen, um die Funktionsfähigkeit bei unterschiedlichen Kapazitätsanforderungen auf die Probe zu stellen: ein vorbeugender eintägiger Stresstest, um alle Kernsysteme per Fernzugriff zu überwachen und zu steuern, falls wirklich niemand ins Unternehmen kommen kann. Die Entwicklung von Anwendungsfällen hilft dabei, den Arbeitsumfang abzuschätzen und zum Beispiel zu klären, wie viel zusätzliche Netzwerkkapazität und wie viele Lizenzen notwendig wären. Ein anderer CIO hat so gravierende Belastungen für den Datenverkehr festgestellt, dass er die Anweisung ausgegeben hat, die gesamte Kommunikation nur noch über Audiokanäle zu führen und nicht mehr über Videokonferenzen.

Zu guter Letzt müssen CIOs gemeinsam mit ihren Kollegen aus anderen wichtigen betrieblichen Funktionen die Systemanforderungen bewerten und sich auf Veränderungen und Supportanforderungen vorbereiten. Im Zuge der Virtualisierung der Organisation können CIOs zum Beispiel auch die Lohnbuchhaltung einem Stresstest mit unterschiedlichen Szenarien unterziehen, um sicherzustellen, dass die Mitarbeiter bezahlt werden.

7. Verlagerung der Geschäftsprozesse ermöglichen. Die besondere Belastung des Systems geht von bestimmten Kanälen aus: Callcenter, Helpdesk, Websites und Apps für Verbraucher. McKinsey hat vor drei Wochen in einer Befragung von chinesischen Konsumenten herausgefunden, dass die Onlinedurchdringung insbesondere in Kategorien mit einer höheren Kauffrequenz

deutlich gestiegen ist (+15 bis 20 Prozentpunkte)². In Italien ist der Onlinehandel seit der letzten Februarwoche um 81 Prozent gestiegen.³

CIOs sollten Websites und Apps für Verbraucher durch Kapazitätserweiterungen auf eine höhere Nutzung vorbereiten und im Kundenservicebereich Selbstbedienungstools und IVR-Systeme einführen (IVR: Interactive Voice Response). Sie können auch mehr Leitungen bereitstellen, die eigens für Covid-19-Anrufe reserviert sind. Außerdem besteht die Möglichkeit, Systeme so auszuweiten, dass auch Kundenservice-Mitarbeiter von zu Hause arbeiten können, und den Helpdesk entsprechend aufzustocken, um das gestiegene Anfragevolumen zu bewältigen. CIOs sollten Helpdesk- und Callcenter-Anfragen sortieren, auf Muster untersuchen und prüfen, ob zusätzliche Maßnahmen erforderlich sind.

Die weitere Entwicklung antizipieren

8. In den wichtigsten Punkten den Kurs beibehalten.

In außergewöhnlichen Stresssituationen wie dieser kommt schnell die Überlegung auf, Programme zu streichen und zu alten Arbeitsweisen zurückzukehren. Natürlich ist es wichtig, die Prioritäten neu zu sortieren, Ressourcen umzuverteilen und die Entwicklung genau im Auge zu behalten. Ebenso entscheiden ist es aber zu erkennen, dass die aktuelle Krise ein kritischer Wendepunkt und eine Wettbewerbssituation ist. Wir wissen aus früheren Krisen, dass Unternehmen, die nur kürzen und ausharren, schlechter abschneiden als solche, die sowohl kürzen als auch gezielt und mit Bedacht investieren.

CIOs müssen auch die Zeit nach der Krise im Blick haben und an ihren übergeordneten Transformationszielen festhalten, zum Beispiel an Programmen in den Bereichen Daten, Cloud und Agile. Die Umstellung auf die Cloud bietet die nötige Flexibilität, um die aktuellen Spitzen sowie die veränderten Anforderungen von Mitarbeitern und Kunden schnell und kosteneffizient zu bewältigen. Das Ziel muss für CIOs darin bestehen, die Krise nicht nur zu überstehen, sondern gestärkt aus ihr hervorzugehen.

Aus diesem Grund ist es wichtig, dass CIOs an Initiativen und Programmen festhalten, die dem Unternehmen zu einer stärkeren Technologieorientierung verhelfen können.

9. Kundenfokus beibehalten. Aufgrund der hektischen Bemühungen, den Geschäftsbetrieb aufrechtzuerhalten, können Unternehmen schnell die Kunden aus den Augen verlieren. Deren Verhalten verändert sich momentan radikal – in vielen Fällen steigen sie auf digitale Kanäle um. Dieses neu erlernte Verhalten dürfte in Teilen auch

nach der Krise bestehen bleiben; das haben wir nach der SARS-Epidemie gesehen, als der Onlinehandel in China regelrecht explodierte.

Gleichzeitig dürfte ein Nachfragestau entstehen, der sich nach der Krise entladen dürfte. McKinsey hat in einer Umfrage unter chinesischen Verbrauchern erfahren, dass sie die allgemeine konjunkturelle Erholung nach Covid-19 optimistisch beurteilen; über 80 Prozent von ihnen gehen davon aus, dass sie nach der Viruskrise genauso viel einkaufen wie zuvor oder sogar mehr. Dabei ist es erheblich wahrscheinlicher geworden, dass sie weiterhin über digitale Kanäle konsumieren.

CIOs sollten Investitionen beschleunigen, die ihren Unternehmen einen Wettbewerbsvorsprung verschaffen können. Der CIO eines Fintech-Unternehmens im Bereich Onlinezahlungen nutzte die Gelegenheit, um das Produkt des Unternehmens aggressiv zu testen und zu vermarkten; wenn sich das Produkt jetzt nicht erfolgreich skalieren lässt, wann dann? CIOs müssen CEOs dabei unterstützen, neue technologiegestützte Geschäftsmodelle zu konzipieren und schnell umzusetzen; Lebensmittelläden werden zum Beispiel Onlineshops und Lieferdienste für betroffene Bevölkerungsgruppen einrichten müssen.

10. Die Auswirkungen der „neuen Normalität“ verstehen.

Die wirtschaftlichen Folgen von Covid-19 sind zwar noch nicht annähernd klar, aber wir gehen davon aus, dass nach der Krise nicht alles genauso weitergeht wie vorher. Die geschäftlichen Auswirkungen von Covid-19 werden CIOs zwingen, die Kosten zu senken, insbesondere auf kurze Sicht. Dazu gehört auch, feste ungenutzte Kapazitäten auf den Prüfstand zu stellen und Initiativen zurückzustellen. Daneben sollten CIOs bei der Bewältigung der negativen wirtschaftlichen Folgen dieser Pandemie auch nach Möglichkeiten suchen, die Produktivität zu steigern.

Vor allem werden CIOs klären müssen, was diese Verschiebungen bedeuten und wie das neue technologiebasierte Betriebsmodell aussehen kann. Manche CIOs denken darüber nach, die veränderten Arbeitsmodi zu nutzen, um neue Verhaltensweisen zu etablieren, zum Beispiel bei internen E-Mails keine Anhänge mehr zuzulassen und die Kommunikation über Slack abzuwickeln. Einige sehen auch die Chance, bessere Verfahren für das Entgegennehmen von Arbeitsaufträgen und für das Nachfragemanagement zu etablieren, um in Krisen oder bei Kapazitätsengpässen den Fokus auf die wichtigsten und wertvollsten Tätigkeiten zu legen. CIOs haben die Chance, Innovationsführer zu werden, statt einfach nur die negativen Folgen wirksam zu managen.

² McKinsey-Umfrage unter 1.249 Menschen in 46 Städten in China, Februar 2020.

³ Expert Calls: „#Coronavirus Nuovi dati sulle vendite della gdo in store e online“, GDOWeek, 6. März 2020, gdoweek.it.

Wie Unternehmen auf die neuen Anforderungen von Mitarbeitern und Kunden reagieren, dürfte ihre Wettbewerbsfähigkeit auf Jahre hinaus prägen.

Wir wissen, dass es vielerorts erst noch schlimmer wird, bevor Besserung in Sicht ist, und es gibt noch viele Fragezeichen. Aber wir sind überzeugt davon, dass CIOs, denen es gelingt, effektiv zu managen und zu führen, jetzt glänzen können.

Aamer Baig ist Senior Partner in Chicago, **Klemens Hjartar** ist Senior Partner im Kopenhagener Büro und **Steve Van Kuiken** ist Senior Partner in New Jersey.

Die Autoren bedanken sich bei Robert Levin und Rahil Jogani für ihren Beitrag zu diesem Artikel. Sie danken außerdem Ritesh Agarwal, Alessio Botta, Rob Cain, Isha Gill, James Kaplan, Gérard Richter, Kate Smaje, Marc Sorel, Hugo Sarrazin, Kevin Wei Wang und Rodney Zimmel für die Erkenntnisse, die sie beigesteuert haben.

Copyright © 2020 McKinsey & Company. Alle Rechte vorbehalten.