Aus der Krise in die Zukunft

Andreas Baresel

Wirtschaftsinformatik & Management 2020 • 12 (4): 240–245

<https://doi.org/10.1365/s35764-020-00277-9>

Online publiziert: 27. Juli 2020

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2020

Als im Frühjahr 2020 das neuartige Coronavirus die Welt fest im Griff hatte, zeigten sich schnell die Stärken, aber auch die Schwächen der IT vieler Unternehmen. Jetzt gilt es, mit den Erfahrungen dieser Ausnahmesituation die Roadmap für die Zukunft festzulegen.

Im ersten Moment sahen sich CIOs vor allem mit technischen Infrastrukthemen konfrontiert: der Beschaffung von Hardware, der Ausrollung der nötigen Software wie zum Beispiel Kollaborationslösungen oder dem Aufbau von performanten Verbindungen etwa über ein sogenanntes „virtuelles privates Netzwerk“ (VPN), das eine sichere Kommunikation etwa mit Mitarbeitern im Homeoffice ermöglicht. Diese Themen waren essenziell, damit Mitarbeiter aus dem Homeoffice weiterarbeiten konnten.

Diese Business Continuity konnte in den meisten Unternehmen gewährleistet werden und hat sich bewährt. Im Zuge dieser Corona induzierten, ungeplanten Homeoffice-Fallstudie haben sich jedoch auch sehr deutlich Lücken und Schwächen gezeigt. Für CIOs gilt es nun, diese Lücken zu analysieren und ihre IT-Governance auf die neue Normalität auszurichten.

IT-Governance und Homeoffice: Anpassung an die neue Zeit

Nie zuvor sahen sich so viele Unternehmen über alle Branchen hinweg mit dem Thema Homeoffice konfrontiert wie aktuell. Laut Branchenverband Bitkom arbeitet sogar jeder fünfte Berufstätige erstmals im Homeoffice [1]. Das bedeutet auch, dass in vielen Unternehmen das Thema Homeoffice nicht integraler Bestandteil der IT-Strategie war, sondern allenfalls ein Thema unter vielen. Es ist daher jetzt essenziell, die IT-Strategie auf das Homeoffice auszuweiten und dieses Arbeitsmodell zu einem festen Bestandteil derselben zu machen. Mussten sich CIOs zunächst stark mit der funktionalen Ebene beschäftigen, sollte es nun um strategisch übergreifende Themen wie Governance und Compliance-Richtlinien gehen.

Security im Homeoffice: Von der Übergangslösung zur Einbindung in die IT-Strategie

Security im Homeoffice ist ein zentrales Thema für CIOs. Das Thema hat zwei Aspekte: zum einen die technische Seite, wie zum Beispiel sichere Authentifizierung und Verbindungen und zentrale Einspielung von Softwareupdates und -patches. Zum anderen ist aber auch das Security Mindset entscheidend für den Erfolg, denn technische Maßnahmen können nur bedingt schützen, wenn Mitarbeiter als Einfallstor dienen.

Durch die Dringlichkeit der Coronasituation sind Securitythemen teilweise vernachlässigt worden. Schnelle, funktionierende Lösungen hatten zunächst einmal Vorrang und die Verantwortung für die Cybersecurity im Homeoffice lag teilweise beim Mitarbeiter. Eine entsprechende Schulung der Mitarbeiter erfolgte jedoch meistens nicht. Das wissen auch Kriminelle, die die ungewohnte Situation auszunutzen versuchen und vermehrt unter anderem Phishing-Attacken starten.

Andreas Baresel (✉)

ist seit Oktober 2018 Mitglied des Vorstands (CPO) der DATAGROUP SE und für das Ressort Produktion verantwortlich. Seine Aufgabe ist die übergreifende Leitung und Koordination der einzelnen Service-Fabriken innerhalb des Konzerns. Nach seinem Studium der Betriebswirtschaftslehre hatte Andreas Baresel verschiedene leitende Positionen mit den Schwerpunkten Business Development und Portfolio-Entwicklung im Bereich IT-Consulting und Managed IT-Services inne. Andreas Baresel kam 2006 mit dem Kauf der DATAGROUP Business Solutions GmbH (ehemals Consinto GmbH) ins Unternehmen und ist seit 2016 Geschäftsführer der DATAGROUP Business Solutions GmbH.

Sara.Gebhardt@datagroup.de

Stuttgart, Deutschland

Zusammenfassung

- Der schnelle Gang ins Homeoffice hat funktioniert, allerdings haben sich deutlich Schwächen und Lücken bei IT-Infrastruktur und IT Governance gezeigt.
- Diese gilt es nun für CIOs zu analysieren und zu beheben: von der Security über die Migration in die Cloud.

Kernthese 1

Eine kontinuierliche Analyse von IT-Infrastrukturkomponenten und entsprechende iterative Anpassung ermöglicht einen effizienteren, sichereren und kostenreduzierten Betrieb.

Die Bedeutung des richtigen Security Mindsets ist daher nicht zu unterschätzen und hier müssen Unternehmen deutlich nachziehen. Das reicht von Passwortrichtlinien über eine sichere, aber intuitive Authentifizierung bis hin zu konkreten Punkten wie Anleitungen zur Verschlüsselung des heimischen WLAN-Netzes.

Zentrale und übergreifende Konzepte

Im ersten Moment wurde viel versucht, um die Lösung zu finden, die in der aktuellen Situation für Unternehmen funktioniert. Es wurden neue Kommunikations- und Kollaborationslösungen ausgerollt oder vermehrt auf die Cloud gesetzt. Das trägt zu einer Fragmentierung der IT bei. Um jedoch Sicherheit und Effizienz zu gewährleisten, ist es wichtig, nun zentrale, übergreifende Konzepte zu entwickeln.

Das bedeutet zum Beispiel ein zentrales und standortunabhängiges Endgerätemanagement, sodass diese zuverlässig von der Unternehmens-IT aus mit den notwendigen Patches versorgt werden können. Mobile-Device-Management bekommt angesichts der aktuellen Situation eine neue Bedeutungsdimension. Wenn mobile Geräte verloren gehen oder Apps Sicherheitslücken aufweisen und missbräuchlich verwendet werden, gefährdet das nicht nur die Sicherheit des Unternehmens, es können auch personenbezogene Daten öffentlich werden, wodurch Unternehmen gegen die Datenschutz-Grundverordnung der Europäischen Union (DSGVO) verstoßen. Es ist daher entscheidend für Unternehmen, Daten auf Geräten zu schützen. Mit Mobile-Device-Management kann dies erfolgen, zum Beispiel indem Geräte bei Verlust aus der Ferne gesperrt und die darin vorhandenen Daten gelöscht werden. Ein weiterer wichtiger Einsatzzweck ist das Black- beziehungsweise Whitelisting von Apps und Containerlösungen, durch die verhindert wird, dass firmeninterne Daten wie zum Beispiel Kontaktdaten in unautorisierte Anwendungen repliziert werden können.

Wichtig ist aber auch, die vielfältigen Softwarelösungen zu analysieren: Welche haben sich bewährt, welche funktionieren, können aber besser ausgebaut und genutzt werden und welche Lösungen werden nicht oder kaum genutzt und sollten daher zurückgerollt werden? Wo sollten Unternehmen einen externen IT-Dienstleister hinzuziehen, um von dessen Erfahrung und Ressourcen zu profitieren?

Expertenwissen über Dienstleister

Es gibt verschiedene Szenarien, bei denen Unternehmen von einem externen IT-Dienstleister profitieren. So ist es gerade in Zeiten des Fachkräftemangels schwierig, im eigenen Unternehmen die nötigen Fachkräfte und internen Ressourcen aufzubauen, die man benötigt, um die vielfältige Bandbreite an IT-Leistungen, die heute nötig sind, zukunftssicher auszubauen und kontinuierlich zu pflegen.

Um nur ein Beispiel zu nennen: Haben User im Homeoffice IT-Probleme, ist es wichtig, dass sie sich schnell an einen jederzeit erreichbaren Service Desk wenden können, der den nötigen Support liefert, damit sie schnell wei-

terarbeiten können. Ein solcher Service Desk ist für viele IT-Abteilungen nicht leistbar, da sie mit einer Vielzahl an Aufgaben bereits ausgelastet sind.

Doch woran können Unternehmen den für sie richtigen IT-Dienstleister erkennen? Der IT-Dienstleister sollte natürlich die nötigen Fachkräfte und langjährige Erfahrung in dem Bereich haben, den das Unternehmen managen lassen möchte. Es lohnt sich aber auch, darauf zu achten, dass der IT-Dienstleister die nötigen Zertifikate wie zum Beispiel ISO 20000 hat, um standardisierte, qualitativ hochwertige Services zu bieten. Darüber hinaus sollte der Dienstleister auf Augenhöhe verfügbar sein. Gerade im Krisenfall hilft es, wenn man einen schnellen Kontakt herstellen kann und Ansprechpartner in der Region hat.

Migration in die Cloud

Die Cloud ist zum Beispiel ein Bereich, bei dem Unternehmen davon profitieren, Expertenwissen aufzubauen oder von externen IT-Dienstleistern einzukaufen. Denn während der Coronasituation hat sich die Cloud als ein großer Gewinner kristallisiert. Bereits vor Corona ging der Trend in deutschen Unternehmen hin zur Cloud und hybriden Lösungen. In der Krise hat die Cloud ihre Stärken ausgespielt, darunter die schnelle Zubuchung von Ressourcen, die weltweite Verfügbarkeit, schlicht die umfassende Flexibilität.

Auch hier zeigt sich, dass ohne die richtige Expertise und die richtige Strategie viele der Vorteile der Cloud ungenutzt bleiben. Denn um bestmöglich von Cloudlösungen zu profitieren, ist eine durchdachte, auf das eigene Unternehmen angepasste Strategie entscheidend. Hier ist in einigen Unternehmen teilweise noch deutlich Luft nach oben. Ein Lift und Shift der bestehenden IT-Infrastruktur und -Lösungen und die 1:1-Übertragung in die Cloud sind zwar schnell und einfach, lassen jedoch viel Potenzial ungenutzt. Unternehmen können sich hier sogar mit höheren Kosten konfrontiert sehen, entgegen dem Versprechen der Kostenersparnis durch die Cloud und angesichts knapper oder ausgereizter IT-Budgets.

Selbige Budgets sollten ebenfalls auf den Prüfstand kommen. Im Zuge des Aufbaus praktikabler IT-Lösungen wurden viele Cloudbudgets ausgereizt. Hier zeigt sich, dass angesichts der nun bewiesenen und künftig noch steigenden Bedeutung der Cloud für den Unternehmenserfolg, die Budgets zu knapp angesetzt wurden. Der Cloudanteil des IT-Budgets sollte daher so angepasst werden, dass er dieser Bedeutung gerecht wird.

Intensive Analyse als Grundstein

Zentral für die erfolgreiche Nutzung der vielfältigen Möglichkeiten der Cloud ist daher eine Bestandsaufnahme: Was sind die Ziele beim Weg in die Cloud? Möchte man primär Kosten einsparen? Oder spielen auch andere Faktoren eine Rolle, etwa die bessere standortunabhängige Erreichbarkeit oder die Flexibilität, bei temporär gesteigertem Bedarf Ressourcen hinzuzubuchen und anschließend wieder zu reduzieren?

Das Ergebnis dieser Analyse kann je nach Komponente der IT-Infrastruktur unterschiedlich ausfallen. So kann es sein, dass es bei einzelnen Kompo-

Kernthese 2

Homeoffice und die Besonderheiten dieses Arbeitsmodells sollten zum integralen Bestandteil der IT-Strategie gemacht werden.

Kernthese 3

Die Kenntnis der durch die Krise offenbarten Stärken und Schwächen der IT-Infrastruktur ist eine Chance, um Lücken zu schließen und in eine digitale Zukunft zu starten.

nenten für das Unternehmen Sinn macht, diese „on premise“ oder bei einem Private-Cloud-Dienstleister in Deutschland zu belassen, etwa wenn das Unternehmen eine starke Kontrolle über bestimmte Systeme behalten möchte. Bei anderen hingegen bietet es sich an, diese in der Public Cloud zu platzieren, zum Beispiel wenn die Auslastung stark schwankt, die Erreichbarkeit zentral ist oder wenn es sich um eine Lösung handelt, für die nur eine kurze Nutzungsdauer vorgesehen ist wie bei Testsystemen.

Erst nach einer solchen Bestandsaufnahme und Analyse mit klaren Endzielen ergibt sich die Cloudstrategie, die zum eigenen Unternehmen passt. Oft entscheiden sich Unternehmen auf dieser Basis für hybride Modelle, bei denen einzelne Komponenten in der Private Cloud bleiben, während andere in die Public Cloud verlagert werden.

Geändertes Mindset nötig

Ihr wahres Potenzial entfaltet eine Public Cloud nur, wenn Unternehmen sie durchdacht nutzen. Gerade Pay-per-use-Modelle werden selten umfassend oder richtig genutzt, vor allem bei einem 1:1-Shift in die Cloud. Zwar gibt es durchaus Komponenten, die sehr statisch sind, also 365 Tage im Jahr stabil und verfügbar laufen müssen, es gibt jedoch auch viele andere, bei denen dies nicht der Fall ist und die zum Beispiel nur werktags zur Verfügung stehen müssen.

Der Weg in die Cloud ist daher nicht nur eine rein architektonische Veränderung, er erfordert eine Anpassung des Mindsets. Die Bereitschaft, ein System von einem 24 × 7-Betrieb auf eine 5 × 10-Nutzung zu ändern, weil dieses nicht am Wochenende oder bei Nacht benötigt wird, kann Kosten entscheidend einsparen.

Im Idealfall läuft jedes System nur so lange und wird auch nur so lange bezahlt, wie es tatsächlich genutzt wird. Um zu diesem Punkt zu gelangen, ist jedoch viel Arbeit und Expertise nötig. Gerade wenn die Infrastruktur unverändert in die Cloud übernommen wird, sind beauftragte Cloudelemente oft überdimensioniert. Ähnlich wie bei vielen Do-it-yourself-Handwerkern unterscheidet sich das, was im Baumarkt gekauft wird, von dem, was letztendlich genutzt wird, oft gravierend.

Kontinuierliche Prüfung und Optimierung

Empfehlenswert ist deshalb die zyklische Analyse der Nutzung der Infrastruktur und iterative Optimierung und Anpassung. Gerade wenn langsam Routine im neuen Alltag einkehrt, sollten Unternehmen überprüfen, ob alle Cloudkomponenten so genutzt werden wie gedacht, und bei Bedarf nachbessern. Dabei sollten die Verantwortlichen es jedoch nicht belassen, sondern zum Beispiel über ein monatliches oder engmaschiges Monitoring die Nutzung kontinuierlich überwachen.

So können sie schnell feststellen, ob entgegen der ursprünglichen Annahmen einzelne Lösungen nur von einem geringen Prozentsatz der Mitarbeiter genutzt werden oder zu anderen als den angenommenen Zeiten, und diese

schnell anpassen. Denn nur so profitieren Unternehmen wirklich von der Flexibilität der Cloud und den damit einhergehenden Kosteneinsparungen.

Neue Normalität, neue Chancen

Die Krise hat die Stärken und Schwächen der IT-Infrastruktur in Unternehmen sehr deutlich gezeigt. Sie ist aber auch eine Chance, nun diese Infrastruktur zu überprüfen und zu optimieren. Eine solche Analyse und Anpassung der IT-Strategie ist zwar mit einem hohen Arbeitsaufwand verbunden, legt aber die Grundlage für eine umfassendere und vor allem sicherere Digitalisierung von Unternehmen. Die Flexibilität, die jetzt an den Tag gelegt und gewonnen wurde, kann sich als wertvolle Grundlage für einen zunehmend digitalen Geschäftsbetrieb erweisen.

Literatur

[1] Bitkom (2020). <https://www.bitkom.org/Presse/Presseinformation/Corona-Pandemie-Arbeit-im-Homeoffice-nimmt-deutlich-zu>. Zugegriffen: 19.06.2020

Handlungsempfehlungen

- Neben den technischen Sicherheitsgrundlagen auch ein Security Mindset beim Mitarbeiter schaffen
- IT-Governance für das Homeoffice entwickeln
- Cloudmigration nicht 1:1 über Lift & Shift, sondern auf die Unternehmensstrategie und -ziele anpassen