IT als wichtiger Teil der Wertschöpfung

Unternehmensstrategien im digitalen Zeitalter müssen um zentrale Aspekte der Informationstechnologie erweitert werden

von Prof. Dr. Stefan Ruf und Prof. Dr. Nils Herda (Hochschule Albstadt-Sigmaringen)

In Zeiten großer wirtschaftlicher Unsicherheit aufgrund technologischer und gesellschaftlicher Umbrüche steht die klassische Unternehmensplanung vor großen Herausforderungen. Die Informationstechnologie wird ein zentraler Bestandteil der Wertschöpfungskette. Dazu muss allerdings – bereits auf der strategischen Ebene – den Besonderheiten der Digitalisierung Rechnung getragen werden. Der Artikel reflektiert daher aktuelle Fragestellungen rund um die unternehmenskritische IT-Governance, das Risk- und Compliance Management.

Gefragt, welche Schlagworte die aktuelle Unternehmensumwelt und insbesondere das ökonomische Umfeld vieler Wirtschaftsunternehmen derzeit am besten charakterisieren, lautet die Antwort vieler Manager schlicht VUCA: **VUCA** repräsentiert als Akronym die Schlagworte „Volatility" (Volatilität), „Uncertainty" (Unsicherheit), „Complexity" (Komplexität) und „Ambiguity" (Mehrdeutigkeit). Und in der Tat ist die Fokussierung auf diese Schlagworte mehr als nur ein Fingerzeig auf die aktuellen Herausforderungen, die Fach- und Führungskräfte in ihrem aktuellen Handlungs- und Entscheidungskontext zwingend beachten müssen.

Das Charakteristikum **Volatilität** zeigt sich nicht zuletzt an den Börsen über die Preisschwankungen für Aktien, Rohstoffe und Währungen. Etwaige Prognosemodelle über deren zukünftige Verläufe sind selbst für langjährige Börsenexperten mittlerweile sehr schwierig geworden.

Um die aktuelle **Unsicherheit** mit einem Beispiel zu untermauern, wäre alleine der Verweis auf den unsicheren Verlauf der Pandemie Covid 19 sowie die unabsehbaren Auswirkungen auf das Investitions- oder Konsumverhalten ausreichend. Die Prognosen reichen von erneuten umfassenden Lockdowns bis hin zur (hoffnungsgetriebenen) Bewältigung der Pandemie durch erste Impfkandidaten.

„VUCA" charakterisiert das ökonomische Umfeld vieler Wirtschaftsunternehmen.

Längerfristige Überlegungen gipfeln in der Idee, den Bezug von Kurzarbeitergeld bis zu 24 Monate zu ermöglichen. Weitere Unsicherheiten werden durch das politische Umfeld, anstehende Wahlen sowie veränderte Handelsbeziehungen generiert. Gerade das Dauerthema „Brexit" droht zudem gerade in einem ungeordneten Handelschaos zu münden.

Ambiguity steht für Mehrdeutigkeiten und die Problematik mehrfacher, teilweise disjunkter Interpretationsmöglichkeiten von Sachverhalten. Immer wieder – und gerade im aktuellen Umfeld verstärkt – zeigt sich dies im (digitalen) Kaufverhalten von Kunden.

Einerseits erleben wir eine starke Reduzierung der Kaufentscheidung auf den Parameter „Preis", der durch Vergleichsportale über verschiedene Hersteller hinweg eine hohe Transparenz aufweist. Gleichermaßen generieren Kunden-Feedbacks, Online-Bewertungen, virale Kaufempfehlungen starke qualitative Präferenzen für die Kaufentscheidung. Eine erfolgreiche Marktpositionierung im Spannungs-

Foto: pixabay.com - Pexel

Der Stellenwert der IT hat sich stark verändert. Neben ihren rein technischen Funktionen wird sie zum wichtigen strategischen Faktor für den Unternehmenserfolg. ▶

feld der Preis- sowie Qualitätsführer wird in diesem Umfeld immer herausfordernder.

Abschließend sei die **Komplexität** der aktuellen Situation anhand eines Beispiels aufgezeigt: Viele Unternehmen stehen derzeit vor der Entscheidung, ihre IT-Infrastruktur grundlegend zu überdenken und neu zu konzeptionieren. Dies vor dem Hintergrund, dass die gewachsenen Informationssysteme den aktuellen Anforderungen der Digitalisierung, der Plattformökonomie und der Skalierbarkeit kaum mehr gerecht werden. Beispiele für derartige komplexe Projekte sind etwa anstehende Migrationen von SAP-Systemen auf die neue Version S/4 HANA oder die Verlagerung hochgradig vernetzter IT-Services in Cloud-Architekturen, häufig außerhalb Europas.

Die Tragweite und Komplexität dieser Projekte reichen bereits heute weit über fachlich-funktionale Anforderungen hinaus. Weitere Anforderungen an die Informationssicherheit, den Datenschutz die Interoperabilität der neuen IT-Systeme generieren eine Komplexität und eine Wirkung nie gekannten Ausmaßes auf die Um-Systeme wie die Geschäftsprozesse oder etwa auf die Arbeitsplatzgestaltung samt den dafür erforderlichen Kompetenzen.

Die VUCA-Herausforderungen vieler Unternehmen reichen somit weit und betreffen dabei stets die Informationssysteme. Zeit, um vor diesem Hintergrund drei wesentliche strategische Aspekte des IT-Managements auf den Prüfstand zu stellen und aktuelle Paradigmen, Strategien und Entscheidungen im IT-Management kritisch zu hinterfragen.

I. IT-Governance

Fokussierend betrachtet, kann unter IT-Governance die strategische Steuerung der Informationssysteme in Unternehmen und der Verwaltung verstanden werden. Durch die strategische Steuerung wird maßgeblicher Einfluss auf die Informationssysteme genommen und zwar durch die Allokation von Budgets und Ressourcen, wichtige Technologieentscheidungen und das Alignment mit der Geschäftsstrategie.

IT-Governance bezeichnet die strategische Steuerung der Informationssysteme.

Verschiedene grundsätzliche Fragestellungen im Zusammenhang mit der IT-Governance in Wirtschaftsunternehmen drängen sich zum aktuellen Zeitpunkt auf und sind durch das Management auch kritisch zu hinterfragen:

1. Welchen aktuellen Stellenwert genießt die IT im Unternehmen, und wie hat sich die aktuelle Einschätzung in den vergangenen Jahren verändert?
2. Wer führt und steuert aktuell die interne IT-Abteilung, und wer ist für die strategische Ausrichtung verantwortlich?
3. Wie hat sich das Budget der IT in den vergangenen Jahren entwickelt, und in welchen Disziplinen werden die Mittel aktuell, aber vor allem künftig allokiert?

Zur ersten Fragestellung lässt sich festhalten, dass die Bedeutung der IT in den vergangenen Jahren ständig zunahm. Sie hat sich jedoch überwiegend noch nicht durchgängig von einem kostenintensiven Werkzeug hin zu einer wertschöpfenden Unternehmensressource gewandelt. Dennoch wird die aktuelle Bedeutung immer noch häufig mit der gegebenen und wachsenden Abhängigkeit von IT-Systemen und der Notwendigkeit für die Unterstützung und Aufrechterhaltung wichtiger Geschäftsprozesse verwechselt.

Eine gute Übung zum aktuellen Zeitpunkt ist die Beantwortung der Fragestellung, welchen Wertbeitrag denn die IT im eigenen Unternehmen aktuell leistet, aber auch welche Potenziale sich durch die Weiterentwicklung, insbesondere durch eine stärkere Digitalisierung von Prozessen und Interaktionskanälen mit Lieferanten, Kunden und Partnern über integrierte Wertschöpfungsnetzwerke erschließen lassen.

Eine quantitative Messung dieser Wertbeiträge bis hin zum konkreten Umsatzbeitrag oder Kostenziel steigert die Akzeptanz und liefert Antworten auf die künftige Allokation von Ressourcen und Mittel im Unternehmenskontext. Wichtige Hinweise auf die Feststellung und Ermittlung differenzierter Wertbeiträge liefert etwa die neue Version der ITIL, einer Management-Richtlinie für das IT-Service-Management in Unternehmen in seiner neuen Version 4.0.

Ebenfalls kritisch können sich Manager derzeit aktuell mit der Fragestellung auseinandersetzen, wer denn die IT-Abteilungen derzeit führt und steuert. Hier reicht das Spektrum von altgedienten Führungskräften, die als „Leiter EDV" oder „Leiter IT/Organisation" fungieren bis hin zu jüngeren ▶

Führungskräften, die als „Chief Digital Officer" (CIO) bezeichnet werden und neben der technisch-organisatorischen Perspektive mitverantwortlich für die digitale Geschäftsentwicklung zeichnen.

Diese enorme Bandbreite gibt einen Hinweis auf den Stellenwert, den Wertbeitrag sowie die Integration der IT im Geschäftsmodell der Unternehmung. Nicht selten korrelieren die Aufgabengebiete auch mit entsprechenden (zusätzlichen) Budgets, die für die explizite Investition in innovative Technologien und Plattformen dediziert sind.

Dies führt zur letzten Frage, die sich Unternehmer und Manager im Kontext der IT-Governance stellen können und müssen: Dem Budget für die IT. Zunächst erfordert dies die gedankliche Flexibilität, die (volatilen und hoffentlich kurzfristigen) Kostendeckel und Kostenbremsen der aktuellen Situation nicht zu berücksichtigen und eine bereinigte Betrachtung der IT-Budgets der vergangenen zehn Jahre kritisch zu reflektieren.

Über drei Viertel des IT-Budgets fließen in den Erhalt und Betrieb der Informationssysteme.

Dabei können verschiedene Betrachtungsdimensionen angestellt werden: Zunächst kann die absolute Höhe der IT-Budgets beobachtet und bewertet werden. Hier sind Leitfragen zu beantworten, z.B. wie hat sich das Budget proportional zum (erwarteten) Wertbeitrag entwickelt? Und waren die bislang getätigten Mittel ausreichend, um erforderliche Investitionen in zukunftsorientierte Technologien, die Weiterbildung der Mitarbeiter oder auch die Abwicklung zielführender Projekte, – wie etwa die Einführung von Business Intelligence-Systemen oder die notwendige Bereinigung von Stammdaten – zu realisieren?

Ein weitere Leitfrage wäre, welcher Anteil des Budgets tatsächlich für Projekte, für das Change Management (Umgestaltung) und für Innovationen effektiv zur Verfügung steht und damit den Wertbeitrag der IT für das Unternehmen nachhaltig zu stärken vermag. Befragungen bei IT-Leitern im Mittelstand legen aktuell nahe, dass zwar Verschiebungen zu Gunsten von innovativen Vorhaben stattgefunden haben, aber immer noch deutlich über drei Viertel des Gesamtbudgets für den Erhalt und den laufenden Betrieb der vorhandenen Informationssysteme aufgewendet werden müssen, womit sich der tatsächlich Spielraum entscheidend verengt.

II. IT-Compliance

Eine häufig ungeliebte, aber nicht minder wichtige Disziplin des IT-Managements stellt die IT-Compliance dar. Hierunter versteht man den Betrieb und die systematische Entwicklung aller Informationssysteme im Unternehmen in der Übereinstimmung mit rechtlichen Vorgaben, vertraglichen Absprachen, weiteren Regularien oder auch freiwilligen Selbstverpflichtungen.

Selbstverständlich werden viele Unternehmer im Brustton der Überzeugung die Auskunft geben, dass der Betrieb ihrer IT-Systeme und die Verarbeitung von Informationen in Übereinstimmung mit allen Vorgaben erfolgt. Wie komplex aber dieses Unterfangen sein kann und warum ein regelmäßiger kritischer Blick auf die Compliance-Aspekte der ▶

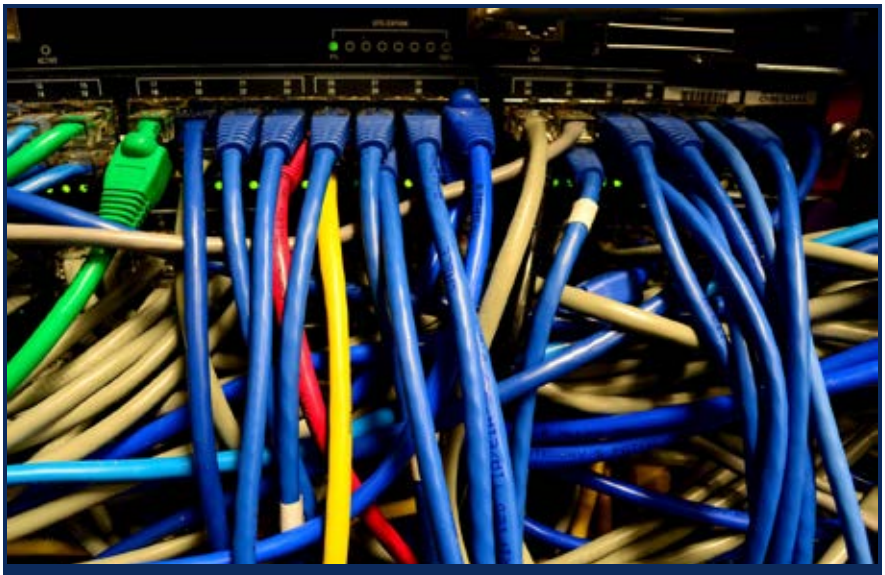

Foto: pixabay.com - ElasticComputeFarm

Meist ist die IT noch immer kostenintensives Werkzeug und hat sich noch nicht durchgängig zur wertschöpfenden Unternehmensressource gewandelt.

Informationssysteme lohnt, sollen zwei Beispiele der aktuellen Unternehmenspraxis verdeutlichen. Erstens die Implikationen der aktuellen EU-Datenschutzgrundverordnung sowie zweitens die Problematik der korrekten Lizenzierung unternehmensweit eingesetzter IT-Software.

Seit der Einführung der neuen EU-Datenschutzgrundverordnung haben Unternehmen vielfältige und aufrichtige Anstrengungen unternommen, die Verarbeitung von Information in Übereinstimmung mit den neuen Gesetzgebungen vorzunehmen.

Eilig wurden häufig interne und externe Datenschützer bestellt, die über längere Zeiträume informationsverarbeitende Prozesse kritisch analysiert haben, notwendige Verfahrensbeschreibungen erstellten und im Extremfall auch Empfehlungen über das Verbot der weiteren Verarbeitung spezifischer personenbezogener Informationen ausgesprochen haben. All diese Bemühungen haben Unternehmen bislang – von wenigen Ausnahmen abgesehen – vor empfindlichen juristischen Folgen und hohen Strafzahlungen bewahrt.

Bereits immer schon kritisch und nicht immer durchgängig transparent war die Verarbeitung von Daten im Auftrag Dritter, die sogenannte Auftragsdatenverarbeitung, insbesondere wenn außerhalb des EU-Rechtsgebiets durchgeführt. Gerade bei der Verarbeitung oder Speicherung von Daten in Cloud-Architekturen großer US-amerikanischer Konzerne war die datenschutzkonforme Informationsverarbeitung häufig Gegenstand kontroverser Diskussionen – wenn auch zumindest durch das Privacy Shield Abkommen gedeckt, das es über Absprachen ermöglichte, personenbezogene Daten zu schützen, die aus einem Mitgliedsstaat der EU in die USA übertragen werden.

Foto: pixabay.com - Gerd Altmann

Der Titel „Leiter EDV" oder „Leiter IT/Organisation" wird zunehmend vom jüngeren Fachexperten, dem sogenannten „Chief Digital Officer (CDO)" abgelöst.

Im Rahmen der DSGVO wurden viele Anstrengungen unternommen, um die neue Gesetzgebung zu erfüllen.

Doch gerade dieses Abkommen wurde im Juli 2020 aufgekündigt: Mit Urteil vom 16. Juli 2020 erklärte der Europäische Gerichtshof den Durchführungsbeschluss (EU) 2016/1250 der Kommission vom 12. Juli 2016 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes für ungültig.

Datenschutzrechtlich Verantwortliche können sich nun nicht mehr länger bei Datentransfers zu Verantwortlichen oder Auftragsdatenverarbeitern mit Sitz in den Vereinigten Staaten – die sich selbst nach dem EU-US Privacy Shield zertifiziert haben – auf die Angemessenheit des Datenschutzniveaus gemäß Artikel 45 DSGVO berufen.

Eine weitere Thematik mit aktueller Brisanz ist der Betrieb von Informationssystemen auf Basis gültiger Lizenzvereinbarungen. Zunehmend komplexe und „interpretierbare" Lizenzmodelle auch großer Software-Hersteller bieten zunehmend Angriffsflächen für den lizenzkonformen Betrieb der Informationssysteme.

Zunehmend zeigen aber externe Audits durch beauftragte Revisoren und Prüfer erhebliche Abweichungen zwischen lizenzierter einerseits und bezahlter sowie effektiv genutzter Software andererseits. Befeuert haben dies eine Vielzahl neuer Cloud-basierter IT-Anwendungen, die zusätzliche Software ▶

und Funktionen nahezu beliebig (nach oben hin) skalieren und die auf Knopfdruck aktiviert werden können. Nicht immer ist den involvierten Benutzern in diesem Moment klar, welche zusätzliche Funktionalität in der Software freigeschaltet und genutzt wird, die aber dann nicht mehr durch die derzeitige Lizenzvereinbarung gedeckt ist.

III. IT-Risk und IT-Risikomanagement

Als letzte der drei wichtigen Disziplinen im IT-Management sei hier abschließend das Thema der IT-Risiken adressiert sowie das der einschlägigen Managementsysteme, die die proaktive oder reaktive Risikosteuerung zum Ziel haben. Grundsätzlich kann konstatiert werden, dass dem Thema der IT-Risiken deutlich mehr Bedeutung zugemessen wird als noch vor wenigen Jahren. Die Sensibilität für den Verlust von Informationen, die Sabotage von IT-Systemen, Hacking- oder Social Engineering-Angriffen hat die Wahrnehmungsschwelle auch des Managements und der Eigentümer erreicht.

Der Gesamtschaden durch Angriffe auf IT-Systeme liegt bereits bei über 100 Mrd. Euro jährlich.

Allerdings kann hier kritisch hinterfragt und als Impuls an die Management- sowie Geschäftsführungsebene vermittelt werden, ob die bisherigen Maßnahmen und Vorkehrungen für die IT-Sicherheit auch wirklich ausreichend sind. Ausreichend vor dem Hintergrund, dass mittlerweile ein Großteil geschäftskritischer Prozesse direkt von der Verfügbarkeit und Funktionsfähigkeit von IT-Systemen abhängig geworden sind. Hier muss analysiert werden, wie lange das Unternehmen Kunden-, Partner- oder Lieferantenbeziehungen tatsächlich aufrechterhalten kann, wenn die zu Grunde liegenden Informationssysteme nicht mehr verfügbar sind oder aufgrund von Sabotage, Hacking oder Anwenderfehlern eine Integrität der Verarbeitung nicht mehr sichergestellt ist.

Aufhorchen lassen immer wieder Studien, die das Ausmaß der Angriffe auf IT-Systeme deutscher Unternehmen dokumentieren, z.B. der Lagebericht des Bundesamtes für Sicherheit in der Informationstechnik für das Jahr 2019. Hier wurden Schadenshöhen durch IT-Angriffe festgestellt, die sich im Einzelfall auf bis zu 40 Mio. Euro durch einen gezielten Ransomware-Angriff (Erpressung durch Verschlüsselung von Daten) beliefen.

Auch die Gesamtschäden liegen nach Informationen des Branchenverbandes BITKOM nunmehr bei bereits über 100 Mrd. Euro jährlich für die deutsche Wirtschaft. Zwei Jahre zuvor betrug das Schadenspotenzial lediglich 55 Mrd. Euro. Ein Negativtrend ist somit klar erkennbar.

Fazit

Aus der Perspektive der Unternehmensführung sind folgende Fragestellungen vor dem Hintergrund einer strategischen Unternehmensführung zu reflektieren:

1. Gibt es eine aktuelle und realistische Einschätzung im Unternehmen über akute IT-Risiken und die aktuelle Gefährdungslage und können die Risikopotenziale im Hinblick auf die Schutzziele Integrität, Verfügbarkeit und Vertraulichkeit informationsverarbeitender Prozesse abgeschätzt werden?

2. Korrespondieren die Risikomanagementsysteme – die Ressourcen und Kompetenzen der Mitarbeiter abbilden – mit den Risikopotenzialen? Sind sie geeignet und ausreichend, um die IT-Assets der Unternehmung proaktiv zu schützen, und verfügt man über die erprobte Fähigkeit der zeitnahen Wiederherstellung?

3. Existieren tatsächlich unabhängige und ungefilterte Experteneinschätzungen über die Risikosituation, die spezifische Gefährdungslage sowie die Eignung der Risikomanagementsysteme im Unternehmen? ■

Quellen

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2019.pdf;jsessionid=027BF1A2684626D17457AC5F95093F03.2_cid501?__blob=publicationFile&v=7

https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-100-Milliarden-Euro-Schaden-pro-Jahr

Die Autoren

Prof. Dr. Stefan Ruf
Professor für Betriebswirtschaftslehre
rufs@hs-albsig.de

Prof. Dr. Nils Herda
Professor für Wirtschaftsinformatik
herda@hs-albsig.de