

IT hinterfragen und besser machen (lassen)

Dr. Carl Stolze

6. June 2022

drcs82

drcs82.de

IT hinterfragen und besser machen (lassen) – auch als Nicht-Techie

Dieses Whitepaper gibt Führungskräften **Leitfragen** an die Hand, um die **eigene IT besser zu verstehen**, zu **hinterfragen** und **weiterzuentwickeln**. Das Dokument lehnt sich dabei an ein bereits erfolgreich in mehreren Unternehmen angewendetes Vorgehen an.

Autor: Dr. Carl Stolze (carl.stolze@drcs82.de, drcs82.de/contact)

Version: 1.0 vom 06. Juni 2022

Hinweis: Dieses Dokument wurde nach bestem Wissen und Gewissen zusammengestellt. Dennoch können Fehler und/oder Unschärfen nicht ausgeschlossen werden. Über einen kurzen Hinweis hierzu freue ich mich.

Muss ich mich auch noch mit sowas beschäftigen?

Informationstechnik (IT) bildet die **Blutbahn** jedes Unternehmens und jeder Organisation in der heutigen Zeit. **Ohne IT geht nichts**. Gleichzeitig kann und muss nicht jede Person ein "Techie" mit tiefem IT-Wissen sein. Gerade in der Führung von kleinen und mittleren Unternehmen oder Organisationen ist selten eine dedizierte IT-Leitung vorgesehen oder existiert gar eine IT-Abteilung.

Selber machen oder machen lassen? Die Fragen sind grundsätzlich gleich. Also hier **keine Scheu** haben auch **Dienstleistern** einmal **auf den Zahn zu fühlen**. Das kann im ersten Moment auf Verwunderung stoßen ("Wir machen das schon richtig", "Vertrauen Sie uns nicht mehr?"). **Langfristig** ist der **Nutzen** jedoch enorm und die Zusammenarbeit wird vielfach **für beide Seiten klarer und angenehmer**.

Stellen Sie sich als **Analogie** vor Ihre **IT** wäre Ihr **Haus** was an dem gerade gebaut wird. Bei einem Haus würden Sie Handwerker oder Architekten sicherlich **nach einem Plan fragen** und auf der Baustelle auch einmal **vorbeischaun**. Oder sogar einen externen Bausachverständigen das Vorhaben begleiten lassen.

Gleichermaßen können Sie auch einen **sachkundigen IT-Experten als Begleiter** engagieren (bspw. über Freelancer-Portale wie *Malt* oder über Netzwerke von IT-Spezialisten wie *Fratch*, oder direkt mich).

Was machen wir mit IT grundsätzlich?

Bevor es an die eigentliche Technik geht, sollte der Umgang mit **IT grundsätzlich betrachtet und reflektiert** werden. Dabei sind keine langen Ausarbeitungen notwendig. Oft reicht es schon einfach in wenigen Sätzen einmal aufzuschreiben, wie der Status Quo ist.

Dabei gibt es **zwei Perspektiven** für die Fragen: Die der Unternehmensleitung und die der Verantwortlichen für die IT. Verantwortlich kann dabei jemand intern in der eigenen Organisation sein (manchmal auch einfach eine Person nach dem "Mach Du das mal bitte"-Prinzip). Oder es handelt sich um einen Dienstleister, wie ein Systemhaus oder einen bestimmten Softwareanbieter.

Daher hier die grundlegenden Fragen zum IT-Einsatz:

| Themenfeld | Unternehmensleitung | IT-Verantwortliche(r) |
|--------------------------|---|---|
| Kerngeschäft | Womit verdient das Unternehmen wirklich sein Geld (Geschäftszweck)? Wie ist das Geschäftsmodell? | Ist die IT Teil des echten Kerngeschäfts? |
| Strategie | Sind im Zeitraum der kommenden drei Jahre wesentliche Veränderungen (Prozesse, Dienstleistungen, Produkte, Organisation) oder Erweiterungen des Unternehmens geplant? | Welche Aktualisierungen oder Veränderungen der Abläufe oder der technischen Landschaft (Hard- und Software) sind geplant? |
| | Wie werden Unternehmens und (langfristige) IT-Planung abgestimmt? | Gibt es eine definierte und aufgeschriebene IT-Strategie und ist diese mit der Geschäftsstrategie abgestimmt? |
| Geschäftsprozesse | Was ist die Wertschöpfungskette im Kerngeschäft? | |
| | Welche Geschäftsprozesse | Welche Geschäftsprozesse |

| | | |
|-----------------------------------|---|--|
| | sind aus Unternehmenssicht am wichtigsten? | werden von der IT am stärksten wahrgenommen? |
| Prozessunterstützung | Gibt es ein inhaltliches Kernsystem (bspw. SAP, Oracle, Sage, eigene Entwicklung) bei den Anwendungen im Unternehmen? | Gibt es ein technisches Kernsystem bei den Anwendungen im Unternehmen? |
| | Welche Anwendungen sind die wichtigsten im Arbeitsablauf? (eigene Einschätzung) | Welche Anwendungen sind die wichtigsten im Arbeitsablauf? (eigene Einschätzung) |
| | Handelt es sich bei dieser Software um Standard- oder Individualsoftware? | Handelt es sich bei dieser Software um Standard- oder Individualsoftware? |
| | | Ist im Einsatz befindliche Standardsoftware ohne Probleme Release-fähig, d.h. Updates können problemlos eingespielt werden? Oder wurden umfangreiche Modifikationen vorgenommen? |
| Organisation der IT | Wie haben sich die IT-Systeme im Lauf der Zeit bis heute entwickelt? (<i>optional</i>) ¹ | Wie haben sich die IT-Systeme im Lauf der Zeit bis heute entwickelt? (<i>optional</i>) ¹ |
| | Wer ist letztendlich für die IT verantwortlich (Geschäftsführung, formale IT-Leitung, Dienstleister)? | Wer ist letztendlich für die IT wirklich verantwortlich (Geschäftsführung, formale IT-Leitung, Dienstleister)? |
| | Wer betreibt die IT (intern, extern, gemischt)? | Wer betreibt die IT wirklich? |
| | | Wie sind die Entscheidungskompetenzen bezüglich IT wirklich? |
| Mögliche Herausforderungen | Welche für die Arbeit relevante IT-Störungen treten derzeit auf oder sind in der Vergangenheit öfter aufgetreten? | Welche, für den Geschäftsbetrieb relevanten, Störungen treten derzeit auf oder sind in der Vergangenheit öfter aufgetreten? |
| | Wie schätzen Sie die Akzeptanz der IT-Systeme durch die Menschen im Betrieb ein? | Wie schätzen Sie die Akzeptanz der IT-Systeme durch die Menschen im Betrieb ein? |

Wo steckt IT eigentlich überall?

Um die IT sinnvoll zu verstehen und weiterentwickeln zu können, sollte nach dem Grundverständnis geschaut werden **wo IT physisch und logisch zum Einsatz gelangt**. Hierzu sind die nachfolgenden **Fragen** gedacht und je nach konkretem Unternehmen oder Organisation entsprechend **angepasst zu stellen**:

| Themenfeld | Fragen |
|-----------------------------|--|
| Räumliche Verteilung | <p>Wo wird IT eingesetzt (Gebäude, Räume, Büros, Lager, Produktionsstätten, usw.)?</p> <p>Wie ist die räumliche Verteilung der IT, insbesondere von zentralen Server und Netzwerkkomponenten?</p> |
| Serverraum/-schrank | <p>Sind die Serverräume bzw. der Serverschrank besonders gesichert?</p> <p>Liegen die Räume in „gefährlichen“ Lagen (Senken wie Tiefgaragen, staubig, feucht, unterhalb von Siloanlagen etc.)?</p> <p>Wie ist die Stromversorgung für die Server(schränke/räume) abgesichert?</p> <p>Wird der Stromverbrauch für die Server getrennt erfasst (Stichwort „Green IT“)?</p> <p>Was passiert bei einem Strom- oder Internetausfall mit den Servern?</p> |
| Netzwerk | <p>Wie ist die Stromversorgung für zentrale Netzwerkkomponenten gesichert?</p> <p>Wie ist das Netzwerk mit dem Internet verbunden? Welche Bedeutung hat diese Verbindung für das Unternehmen? Kann bei einem Ausfall weiter gearbeitet werden? Wie sind Redundanzen geplant?</p> <p>Gibt es WLAN-Access-Punkte im Netzwerk?</p> <p>Welche Sicherheitsmechanismen werden im Netzwerk eingesetzt (Firewall, Intrusion Detection, Virens Scanner, logische Partitionierung in VLANs, etc.)?</p> |
| IT in der Produktion | <p>Wo und mit welchen Aufgaben wird IT in der Produktion eingesetzt?</p> <p>Welche Systeme könnten die Produktion</p> |

| | |
|---|---|
| | <p>(Ausfall, Gefahr für Leib, Leben und Gesundheit) gefährden bei Fehlfunktionen?</p> <p>Wie sind diese Systeme mit anderen IT-Komponenten verknüpft (physisch und logisch)?</p> <p>Wo und mit welchen Aufgaben wird IT im Labor eingesetzt? Handelt es sich um es Entwicklungs- oder um Prüfaufgaben?</p> <p>Welche Systeme sind notwendig im Labor, um die Kernprozesse im Unternehmen aufrecht zu erhalten (Freigabemechanismen, notwendige Laborwerte etc.)?</p> <p>Wie sind diese Systeme mit anderen IT-Komponenten verknüpft (physisch und logisch)?</p> |
| <p>IT im Labor</p> | |
| | <p>Welche Systeme sind notwendig, um den Bestand des Unternehmens nicht zu gefährden?</p> <p>Wo und wie werden Qualitätsmanagement-Handbücher, Verfahrensanweisungen, Betriebsanleitungen usw. verbreitet und aktualisiert? (IT-gestützt oder Ordner, Ausfallsicherheit etc.)</p> <p>Wie sind diese Systeme mit anderen IT-Komponenten verknüpft (physisch und logisch)?</p> |
| <p>IT in der Verwaltung und Büro</p> | |
| | <p>Welche Systeme sind notwendig, um Lager zu bewirtschaften? (Beispiel: Ist bei Ausfall der Hochregalsteuerung das Hochregallager noch nutzbar?)</p> <p>Wie sind diese Systeme mit anderen IT-Komponenten verknüpft (physisch und logisch)?</p> |
| <p>IT im Lager</p> | |
| | <p>Welche anderen IT-Einsätze gibt es? (Beispielsweise mobile Geräte im Außendienst, Kantinenbetrieb, Buchung Konferenzräume, usw.)</p> <p>Wie sind diese Systeme mit anderen IT-Komponenten verknüpft oder abhängig von diesen (physisch und logisch)?</p> |
| <p>Sonstige IT</p> | |

Allein durch diese Fragen können **Verbesserungspotenziale** erkannt werden. Einerseits vielleicht überflüssige oder **doppelte Systeme**, andererseits zwingt es **Dienstleister** auch **offen zu legen** was wirklich im Einsatz und auch dokumentiert ist.

Wie sicher und verfügbar sind eigentlich die IT und die Daten?

IT soll sicher und verfügbar sein. Die beiden Felder **Sicherheit und Verfügbarkeit** sind dabei extrem **vielschichtig**, so dass diese **Fragen** ein Anfang der Beschäftigung sind.

| Themenfeld | Fragen |
|----------------------|---|
| Verfügbarkeit | <p>Welche Verfügbarkeit ist notwendig für welche Anwendungen (unkritisch, kritisch, unternehmensgefährdend bei Ausfall)?</p> <p>Welche Verfügbarkeit wird für welche Anwendungen real erreicht?</p> <p>Wie wird die Verfügbarkeit von Systemen überwacht?</p> |
| Störungen | <p>Wie werden Störungen neben reiner Verfügbarkeit bemerkt?</p> <p>Wie werden Störungen behoben?</p> |
| Wartung | <p>Wie werden laufende Wartung und Administration durchgeführt? Eher planvoll oder eher ad-hoc nach Bedarf?</p> <p>Sind die notwendigen Fähigkeiten zur Wartung kurzfristig verfügbar (bspw. Personen, Rufbereitschaft, verwendete Software, etc.)?</p> <p>Existiert eine hinreichende Dokumentation?</p> |
| Datenschutz | <p>Wie ist der Schutzbedarf (Vertraulichkeit, Datenverlust, Integrität) welcher Daten in welchen Systemen?</p> <p>Welche technischen Maßnahmen zum Datenschutz sind IT-seitig umgesetzt? (Beispiel: Verschlüsselung Festplatten)</p> <p>Welche organisatorischen Maßnahmen zum Datenschutz sind IT-seitig umgesetzt? (Beispiel: Verwendung personengebundener</p> |

Backups

Accounts)

Wie werden Backups von welchen Daten durchgeführt?

Gibt es ein physisch getrenntes Backup?

Nach welchem Schema wird das Backup durchgeführt?

Wie ist sichergestellt, dass bspw. ein Verschlüsselungstrojaner nicht auch das Backup (nachträglich) verschlüsselt?

Für die einzelnen Aspekte können (und sollten) dann je nach Bedarf spezialisierte Personen herangezogen oder befragt werden. Beispielsweise kann zum Datenschutz auch ein betrieblicher Datenschutzbeauftragter Hinweise geben.

Ergänzend: Branchen-spezifische Aspekte

Bei den Fragen sollten Sie auch immer wieder für Ihr Unternehmen bzw. Ihre Branche **spezifische Aspekte** berücksichtigen.

Hier sind einige selektive Beispiele:

- Finanzdienstleistungen: Regulatorische Anforderungen (u.a. aus KWG, der MaRisk, BAIT, usw.)², Schnittstellen, Dokumentationspflichten
- Lebensmittelproduktion: Chargenzuordnung, Allergene (Rezepturen, Kreuzkontamination im Lager, usw.), Rückverfolgbarkeit, Sensoren/IoT (bspw. Temperatur), spezielle Datenstrukturen für mikrobiologische Analysen
- Gesundheitswesen: Strengerer Datenschutz, Schnittstellen zu Krankenkassen, Abrechnungsstellen, Laboren mit definierten Datenstrukturen, Umgang mit Gesundheitskarten, Bezahlung von individuellen Leistungen (ggf. Anbindung Kartenterminals)
- Bau: Zeiterfassung, Materialerfassung (bspw. mobil auf der Baustelle), Digitalisierung von Plänen (Baunformationssysteme), Besonderheiten Bau Lohn (Schnittstellen zum Steuerberater/Lohnbuchhaltung)

Und so hat **jede Branche spezielle Anforderungen** an die IT. Gerade generalistische IT-Anbieter *können* nicht jede Branche im Detail kennen. Da ist es gut nachzufragen und gemeinsam zu überlegen, wie es passen kann.

Wie die Fragen stellen und Antworten dokumentieren?

Für die Platzierung der Fragen sollte **unbedingt** das **persönliche Gespräch** mit den **Fragen als Leitfaden** gesucht werden.

Ein Versand per E-Mail führt schnell zu Missverständnissen oder unnötigem Aufwand, wenn nicht klar ist wie tief eine Frage beantwortet werden soll. Im Gespräch können dann auch **Rückfragen** gestellt werden oder weitere **Unterlagen** für Details angefordert werden. Dabei sollten die **Antworten** während des Gesprächs **notiert** werden und Gesprächspartnern im Nachgang zur Bestätigung per E-Mail zugesendet werden.

Wie geht es dann weiter?

Die gesammelte Information sollte ein **besseres Verständnis** für die eigene IT **erzeugt** haben. Durch den strukturierten Dialog sollte dabei auch das beidseitige Verständnis für Anforderungen und die gewählte Umsetzung steigen.

Gleichzeitig ist es **teilweise schwer** die Antworten **zu hinterfragen** ohne über entsprechendes IT-Know-How zu verfügen. Spätestens an dieser Stelle sollte ein **sachkundiger Dritter als neutrale Instanz** hinzugezogen werden. Dieser kann die *richtigen* Fragen stellen und *übersetzt* zwischen Geschäftsleitung und IT-Verantwortlichen. Natürlich könnte auch direkt die Erhebung durch diesen Dritten erfolgen.

Für die **Weiterentwicklung** der IT können dann in der Folge konkrete Maßnahmen geplant und grob geschätzt werden. Hierauf aufbauend kann die Geschäftsleitung dann eine **bewusste und informierte Entscheidung** zur Umsetzung treffen.

Über den Autor

Dr. Carl Stolze berät Unternehmen mit dem Schwerpunkt nachhaltiger Einsatz von IT und Digitalisierung. Dabei arbeitet er auf den Ebenen der Strategie, Architektur und in Projekten mit klassischen und agilen Methoden. Mehr Informationen auf drcs82.de.

Über dieses Whitepaper

Diesem Whitepaper liegt die jahrelange Erfahrung in der Beratung von Unternehmen durch Dr. Carl Stolze zugrunde. Immer wieder konnten dabei die selben oder sehr ähnliche Herausforderungen identifiziert werden.

Die allererste Version des Fragenkatalogs entstand dabei bereits 2011/2012 während der Promotionszeit am Lehrstuhl für Informationsmanagement und Wirtschaftsinformatik der Universität Osnabrück. Hier entwickelte Dr. Carl Stolze zusammen mit Dr. Novica Zarvic und Prof. Dr. Oliver Thomas im Rahmen eines Projekts zur *IT-Reorganisationsberatung für KMU* die erste Sammlung von Fragen und erprobte diese erfolgreich bei Unternehmen der Lebensmittelindustrie (unterstützt durch das DIL).

In der Folge konnte der Fragebogen sukzessive erweitert werden. Heute bildet er für interessierte Führungskräfte einen guten ersten Ansatzpunkt um die eigene IT zu hinterfragen und besser zu verstehen, um so Verbesserungspotenziale zu identifizieren.

1. Die optionale Frage nach der Entwicklung hilft, insbesondere gefragt durch einen neutralen Dritten, auf mehreren Ebenen: Neben der technischen Evolution werden mindestens implizit auch organisatorische Entwicklungen oder Herausforderungen sichtbar.
2. KWG = Gesetz über das Kreditwesen (Kreditwesengesetz)
MaRisk = Mindestanforderungen an das Risikomanagement
BAIT = Bankaufsichtliche Anforderungen an die IT