

DER WEG ZU EINER ZUKUNFTSFÄHIGEN IT

6 Dinge, die Sie beim Aufbau Ihrer (internen) IT-
Abteilung beachten sollten

November 2022

Zusammenfassung

Eine zum Unternehmen passende IT-Abteilung wird immer wichtiger um gut auf zukünftige Entwicklungen vorbereitet zu sein. In diesem Whitepaper diskutieren wir die wichtigsten Aspekte, die Sie bei der Umsetzung der eigenen IT-Abteilung berücksichtigen sollten.

Dr. Christoph Wienken
christoph.wienken@fly-tech.de

Impressum

fly-tech IT GmbH & Co KG
Winterbrückenweg 58
86316 Friedberg

Telefon: 0821 207111 16
Fax: 0821 207111 10
E-Mail: kontakt@fly-tech.de

Autor
Dr. Christoph Wienken (fly-tech IT GmbH & Co. KG)

Namensbeiträge geben die Meinungen der Verfasser wieder.
Sie entsprechen nicht unbedingt der Auffassung des Herausgebers.

Layout und Verlag
fly-tech IT GmbH & Co KG

Bildnachweis

Nachdruck und Vervielfältigung, auch auszugsweise, nur mit Quellenangabe gestattet.

Friedberg, November 2022
Erste Auflage



Executive Summary

Für die meisten Unternehmen ist IT nicht der Kern der unternehmerischen Tätigkeit. Aber eine funktionierende IT kann Prozesse effizienter machen. Damit ist sie immer ein wichtiger Erfolgsfaktor, der darüber entscheiden kann, wie gut ein Unternehmen im Markt besteht. Das reicht von kürzeren Produktionszyklen, durch reibungslos verfügbare Daten, bis hin zu höherer Mitarbeiterzufriedenheit, dank moderner Arbeitsmodelle mit besserer Work-Life Integration.

Doch die eigene interne IT-Abteilung stellt viele Unternehmen immer wieder vor Herausforderungen. So benötigen der Aufbau und die Weiterentwicklung einer effektiven IT-Abteilung viel Aufmerksamkeit. Einerseits bei der Personalsuche, denn qualifizierte Mitarbeiter im IT-Umfeld sind schwer zu finden und gefragt. Andererseits beim Etablieren von funktionierenden Prozessen im Unternehmensalltag.

In der Konsequenz ist eine optimale IT-Betreuung durch eine internen IT-Abteilung für viele Unternehmen schlicht zu teuer und sie begnügen sich mit abgespeckten Lösungen in der Umsetzung - mit schlecht vorhersagbaren Konsequenzen für die Zukunftsfähigkeit und die IT-Sicherheit des Unternehmens.



Wann haben Sie sich das letzte Mal Gedanken über die IT Ihres Unternehmens gemacht? Für viele Unternehmer und Führungskräfte ist IT etwas, das nur dann in den Fokus kommt, wenn sie nicht funktioniert. Wenn beispielsweise das Endgerät nicht ausreichend Performance für die gewünschte Anwendung bietet. Oder ein Server ausgefallen ist und deshalb der Zugriff auf wichtige Daten nicht mehr möglich ist.

Jedes Unternehmen muss sich daher die Frage stellen, wie es die Funktion der eigene IT sicherstellen will. Und je nach Unternehmensgröße und Selbstverständnis kommen hier sehr unterschiedliche Lösungen in Frage. Das reicht von einem IT-Management „nebenher“, über ein Outsourcen der IT-Themen zu einem Dienstleister bis hin zu einer eigenen IT-Abteilung bestehend aus einem oder mehreren Mitarbeitern. Doch unabhängig von der gewählten Lösung sind dabei immer wieder ähnliche Dinge zu beachten, die wir im Rahmen dieses Whitepapers vorstellen und diskutieren wollen.

1. Unternehmens-IT benötigt IT-Fachexperten

Auch wenn viele Mitarbeiter aus dem privaten Umfeld gewohnt sind, ihre IT selbst umzusetzen und zu administrieren, so führt das im Unternehmensumfeld regelmäßig zu Problemen. Insbesondere die zunehmende Vernetzung von Anwendungen führt dazu, dass die verwendeten IT-Lösungen unbedingt sauber und korrekt implementiert werden müssen. War es früher noch akzeptabel „Work Arounds“ oder Insellösungen zu nutzen, so führt dies heute dazu, dass die Vorzüge der Vernetzung nicht genutzt werden können, oder es hat vielleicht sogar negative Auswirkungen auf die Performance der Anwendungen. Außerdem sind Sicherheitslücken im privaten

Umfeld häufig weniger kritisch als im Unternehmenskontext.

Deshalb ist es sehr wichtig, dass für die kritischsten Fachbereiche auch Expertenwissen im Unternehmen verfügbar ist. Das beinhaltet Hardware-Experten, die sich um eine optimale WLAN-Abdeckung in den Büroräumen kümmern genauso wie Cloud-Spezialisten, welche die Unternehmensdaten überall verfügbar machen und dabei die nötige Datensicherheit im Blick behalten. Um das gewährleisten zu können, ist eine gute Ausbildung und vor allem auch eine regelmäßige Weiterbildung der Experten erforderlich. Und die schiere Menge an unterschiedlichen Themen macht es für einzelne IT-Mitarbeiter quasi unmöglich alle Themen adäquat abzudecken.

In der Konsequenz benötigt ein Unternehmen im Idealfall eine Abteilung aus mehreren Mitarbeitern mit unterschiedlichem Wissen und Erfahrung. Dies ist jedoch meist mit hohen Kosten verbunden. Das wiederum führt dazu, dass viele, insbesondere kleinere, Unternehmen, die eine eigene interne IT-Abteilung betreiben, in diesem Punkt Abstriche in Kauf nehmen müssen.

2. Unternehmens-IT benötigt gute Erreichbarkeit und Vertretungslösungen

Eines haben viele IT-Themen gemeinsam. Wenn ein Problem auftritt und die IT ausfällt, dann geht für die Betroffenen häufig nichts mehr. Für das Unternehmen ist das immer ärgerlich. Aber häufig kostet so ein Ausfall auch noch richtig Geld. Stellen Sie sich vor sie können aufgrund eines Netzwerkausfalls für 24h keine Waren produzieren.



Deshalb ist es wichtig, für unternehmenskritische Prozesse eine gute Erreichbarkeit der IT-Verantwortlichen sicher zu stellen. Denn wenn alles steht, sind kurze Antwortzeiten wichtig. Das führt viele Unternehmen mit eigener IT-Abteilung vor Herausforderungen. Selbst wenn während der normalen Arbeitszeiten eine gute Erreichbarkeit gewährleistet ist, so fehlt außerhalb dieser Zeiten meist eine Betreuung. Hier muss über teure Bereitschaftsdienste eine Abdeckung sichergestellt werden. Und auch wenn die meisten internen IT-Mitarbeiter bereit sind, hin und wieder auch am Wochenende zu unterstützen, so wollen doch die wenigsten jeden Abend und jedes Wochenende auf Abruf bereitstehen.

Das gilt umso mehr für die Urlaubszeit: Befindet sich die interne IT im Erholungsurlaub am anderen Ende der Welt, wird es schwierig zeitnah die IT-Probleme zu lösen. Gleiches gilt auch im Falle einer überraschenden Kündigung des Mitarbeiters oder im (längeren) Krankheitsfall.

Die Lösung der meisten Unternehmen wäre hier auch, die interne IT-Abteilung mit zusätzlichem Personal aufzustocken. Doch häufig sind im Normalbetrieb dafür nicht ausreichend Aufgaben vorhanden und somit ist das ein sehr teures Sicherheitsnetz.

3. Unternehmens-IT benötigt etablierte Prozesse und Abläufe

Eingespielte Prozesse sind der Kern eines jeden erfolgreichen Unternehmens. Durch sie kann eine Produktion skalieren oder optimiert werden. Doch um Prozesse etablieren zu können, müssen die Abläufe regelmäßig auftreten und man benötigt Vertrauen in die

gefundene Lösung, um diese als den neuen Standard einzuführen.

Vor allem bei kleinen und mittleren Unternehmen treten die IT-Themen aber typischerweise nicht so regelmäßig auf, dass sich ein Standardablauf einspielen kann. Jede Störung wird als Einzelfall betrachtet. Daraus resultiert ein wenig einheitliches und kaum optimiertes Vorgehen. Deshalb sind erfahrene IT-Mitarbeiter so wertvoll, weil sie hier auf Prozesswissen aus früheren Tätigkeiten zurückgreifen können. Natürlich kann das Unternehmen mit IT-Prozessberatern einen Grundstock an Prozessen aufbauen, welche die häufigsten Störungsfälle und die optimalen Prozesse zur Problembehebung abdecken. Aber die Optimierung auf das eigene Unternehmen bleibt eine Herausforderung, da die Abstände zwischen den einzelnen Fällen sehr groß werden können. Da hilft meist nur eine gute und detaillierte Dokumentation der Störungen und der entsprechenden Lösungen. Größere IT-Abteilungen verwenden hierzu meist ein Ticketsystem, das die Bearbeitung der IT-Fälle überwacht und gleichzeitig eine fallbasierte Dokumentation ermöglicht.

4. Unternehmens-IT benötigt kalkulierbare Kosten

Die IT-Kosten sind bei vielen Unternehmen ein zentrales Thema. Denn interne IT-Mitarbeiter sind rar und deshalb auch teuer. Und auch bei den Investitionen in Hard- und Software kommen schnell größere Beträge zusammen, die sich unschön auf das Monats- oder auch Jahresergebnis auswirken.

Laut einer Studie von Capgemini aus 2022 besteht das Hauptproblem bei den IT-Kosten häufig allerdings weniger in den akuten Kosten, sondern vor allem auch darin, dass diese meist



überraschend anfallen. Der Server fällt aus und kann nicht mehr repariert werden. Jetzt muss er so schnell wie möglich ersetzt werden. Oder die bestehende Hardware wird durch eine neue Softwareversion nicht mehr unterstützt und muss erneuert werden.

Um trotz dieser spontan auftretenden Notfälle planbar zu bleiben, benötigt es jemanden, der sowohl die Priorität und Dringlichkeit der einzelnen Themen einschätzen kann, aber zur gleichen Zeit auch den Blick auf das zur Verfügung stehende Budget behält. Es braucht einen IT-Koordinator. Doch viele Unternehmen scheuen die Investition in eine solche Stelle und übertragen die Aufgabe dem IT-Mitarbeiter. Oder das Management übernimmt diese Aufgabe als Seitenprojekt. Beide Herangehensweisen sollten aus unserer Sicht allerdings nur kurzfristige Lösungen sein. Denn in einem Fall sucht das Unternehmen unter den sowieso schon rar gesäten IT-Experten die sogenannte „Nadel im Heuhaufen“. Und im anderen Fall versucht das Management mit häufig oberflächlichem IT-Wissen die richtigen Entscheidungen zu treffen.

5. Unternehmens-IT benötigt eine abgestimmte IT-Strategie

Und auch bei der Ausgestaltung der IT-Strategie des Unternehmens fehlt häufig Expertise. Die internen IT-Mitarbeiter haben meist einen stark operativen Fokus. Als Resultat ist die IT-Abteilung in vielen Fällen nur eine Art „Feuerwehr“. Wenn es brennt, muss schnell gehandelt werden. Ansonsten wartet man darauf, dass etwas passiert. Dabei könnten die meisten „Feuer“ gut vermieden werden, wenn man vorab plant und die Weiterentwicklung der IT mit der Unternehmensentwicklung abstimmt.

Für eine zukunftsfähige IT-Strategie ist es deshalb wichtig, die Zukunftspläne des Unternehmens zu kennen und mit zu berücksichtigen. Denn wenn in Kürze eine Expansion des Unternehmens ansteht, so muss sich häufig auch die Unternehmens-IT auf diesen Schritt vorbereiten. Nur dann kommen die möglicherweise anfallenden IT-Investitionen nicht überraschend.

Zusätzlich ist es auch sinnvoll die Unternehmensphilosophie zu berücksichtigen. Ein Unternehmen, das stark auf gut ausgebildete Mitarbeiter angewiesen ist und mit vielen anderen Unternehmen um diese konkurriert, möchte den eigenen Mitarbeitern möglicherweise ein modernes und hybrides Arbeiten ermöglichen. Denn seit der Pandemie hat sich die Prioritäten der Mitarbeitenden verändert. Laut Microsoft Work Trend Index 2022 räumen jetzt 47% der befragten Personen ihrem Familien- und Privatleben eher Vorrang vor der Arbeit ein als vor der Pandemie. Und Grundlage für ein flexibles hybrides Arbeiten ist eine gute IT-Architektur.

Auch wer kritische Daten von seinen Kunden bekommt, möchte sich vielleicht stärker um die eigene IT-Sicherheit kümmern als der Handwerksbetrieb von nebenan. Einfach deshalb, weil die Kunden sich stärker für diese Themen interessieren.

6. Unternehmens-IT benötigt eine effektive IT-Sicherheitskonzepte

Die IT-Sicherheit sollte sowieso immer ein zentraler Punkt der IT-Strategie sein. Und diese wird zunehmend auch für kleiner Unternehmen wichtig. Denn Cyberangriffe beschränken sich schon länger nicht mehr nur auf große Konzerne. Schon so mancher Mittelständler wurde bereits Opfer eines Verschlüsselungstrojaners und von Erpressungsversuchen. Hier hilft es, die eigene



Strategie mit einem unabhängigen Standard zu bewerten und sich beispielsweise an den Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) zu orientieren. Denn immer höhere Mauern um die eigenen Daten und das eigene Unternehmen zu errichten ist in einer vernetzten Arbeitswelt nicht mehr zeitgemäß. Vielmehr gilt es die richtigen Sicherheitskonzepte wie z.B. Zero-Trust Konzepte zu implementieren und damit die Hoheit über seine Daten zu behalten und den Zugriff an bestimmte Kriterien zu knüpfen. Dies erfordert jedoch eine völlige Neu-Ausrichtung bisheriger Sicherheitskonzepte in klassischen Netzwerken und damit IT-Manager, die zusammen mit IT-Architekten arbeiten, die weitblickend agieren.

Zudem werden neben den technischen Lösungen auch organisatorische Maßnahmen wichtiger und die Einführung eines und die Optimierung der internen Prozesse bis hin zur Einführung eines Informationssicherheitsmanagementsystems kann viele Schwachstellen und Angriffspunkte aufdecken und lösen.

Zusammenfassung

Aus der Diskussion der Punkte sieht man, welche vielfältigen Herausforderungen auf die IT-Abteilung der Zukunft zukommen. Eine funktionierende IT bildet immer stärker die Grundlage eines effizient arbeitenden Unternehmens und sollte deshalb den nötigen Fokus und die nötige Priorität bekommen. Für die Unternehmen wird es zunehmend wichtiger für die einzelnen Themen internes oder externes Expertenwissen zur Verfügung zu haben und damit dem Unternehmen die Vorzüge des hybriden Arbeitens zu ermöglichen.

Denn die Flexibilität dieser Arbeitsform wird immer stärker zu einem Unterscheidungsmerkmal zwischen den Unternehmen. Sei es bei der Reaktionsfähigkeit auf Änderungen am Markt oder beim Wettbewerb um die besten Mitarbeiter.



Referenzen

Bundesamt für Sicherheit in der Informationstechnik (BSI) – Lagebericht 2021

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2021.pdf?__blob=publicationFile&v=3

Capgemini – “Studie IT-Trends 2022” <https://www.capgemini.com/de-de/wp-content/uploads/sites/8/2022/08/Studie-IT-Trends-2022.pdf>

Kienbaum – Whitepaper “Future Workplace” https://media.kienbaum.com/wp-content/uploads/sites/13/2021/02/DE_Whitepaper_Future_Workplace_geschuetzt.pdf

Microsoft – “Work Trend Index 2022: Jahresbericht”
<https://clouddamcdnprodep.azureedge.net/gdc/gdcDjZ4e8/original>

Techconsult – Report “Entwicklung der Budgets und Projekte in der IT deutscher Unternehmen”
<https://www.infinidat.com/de/resource-pdfs/techconsult-report-de.pdf>

VOICE Bundesverband der IT Anwender e.V. “IT-Agenda 2022” <https://voice-ev.org/wp-content/uploads/2022/02/VOICE-Metrics-Trendstudie-IT-Agenda-2022-DE-v1-1.pdf>

