IT-Health-Check – IT-Risiken erkennen und die daraus entstehenden Chancen nutzen

Ein stabiles und robustes IT-Umfeld und ein Bewusstsein für die Cyber-Risiken und die begrenzten IT-Ressourcen helfen der Unternehmensführung, verlässliche Informationen bereitzustellen und als KMU am Markt erfolgreich zu sein. Der Artikel zeigt, wie eine objektive, externe Sicht die Unternehmensführung dabei unterstützen kann, sich vor IT-Risiken zu schützen.

Philipp Schweizer
Senior Manager/
IT-Prüfer
Zürich

KMU und deren Inhaber, CIO, Leiterinnen Informatik und weitere IT-Verantwortliche sehen sich heutzutage mit vielen Herausforderungen konfrontiert. Neben der digitalen Transformation und der wachsenden Komplexität stehen auch die IT-Sicherheit und begrenzte IT-Ressourcen (IT-Budgets) weit oben auf der Agenda. Zudem erhöhen in jüngster Zeit die vermehrten Cyberattacken das unternehmerische Risiko. In einem solchen Umfeld ist es wichtig, dass die IT-Risiken bekannt und die Kernprozesse im Tagesgeschäft adäquat an diese angepasst sind.

IT-Risiken erkennen

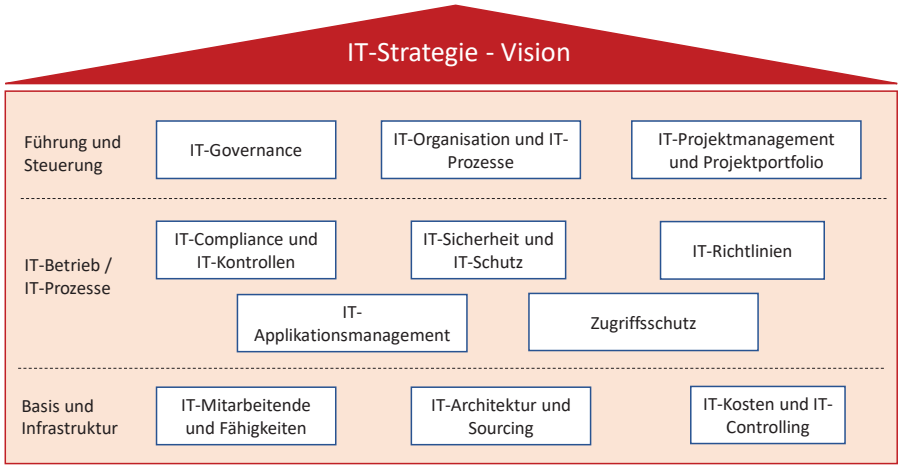
Eine Harmonisierung der IT-Architektur mit gleichzeitiger Digitalisierung bringt auch die Herausforderung von Agilität und einem stabilen Kontrollumfeld mit sich. Oft werden dabei viele grundlegende Risiken nicht oder nicht vollumfänglich berücksichtigt. Eine objektive und externe IT-Risikobewertung, z.B. im Rahmen eines IT-Health-Checks, kann hilfreich sein und einen frischen Blick auf die eigenen Projekte und Herausforderungen bringen. Grundsätzlich lassen sich drei Hauptebenen mit weiteren Fokusthemen identifizieren (siehe IT-Strategie und Vision).

- Führung und Steuerung

  Erfahrungsgemäss ist es für KMU aufgrund oftmals knapper Personalressourcen eine Herausforderung, die Verantwortlichkeiten im Bereich IT genau zu definieren. Gerade bei ERP-Umstellungen ist es wichtig, eine erfolgreiche Datenmigration sicherzustellen. Hierbei werden projektseitig grundlegende Fragestellungen in vielen Fällen nicht angemessen adressiert. Neben der vollständigen und richtigen Datenmigration ist es zentral, die Fachbereiche rechtzeitig einzubeziehen, Projektorganisation und -kontrollorgane, vorgängige Datenbereinigungen, Fehlerbehandlungen sowie Abnahmen nicht aus den Augen zu verlieren und proaktiv zu steuern. Dabei sollten folgende Fragen beantwortet werden:
  - Ist die IT-Organisation passend aufgestellt, um wesentliche Kernprozesse und IT-Projekte adäquat zu unterstützen?
  - Werden Projekte zeitgerecht, im Budget und qualitativ wie gewünscht abgeschlossen?
  - Ist die IT-Strategie auf die Unternehmensstrategie abgestimmt?
- IT-Betrieb/ IT-Prozesse

  Im Rahmen des IT-Betriebs sind u.a. Zugriffsschutz, Funktionentrennung, Berechtigungskonzept und Änderungswesen zu definieren und zu überwachen.
  Hier stellen sich Fragen wie:
  - Sind alle Änderungen und Zugriffe angemessen definiert, freigegeben und kontrolliert?
  - Herrscht ein allgemeines Bewusstsein zu Cyberrisiken, und werden diese überprüft?
  - Sind die Mitarbeitenden entsprechend sensibilisiert und geschult?
- Basis und Infrastruktur

  CIO oder Leiter/innen Informatik sind grundsätzlich für die laufende Infrastruktur sowie deren Performance und Kosten verantwortlich. Zu ihren Hauptthemen gehören folgende Fragen:
  - Nutzt man ein In- oder Outsourcing von Rechenzentren, Services und Dienstleistungen?
  - Sind alle Anwendungen auf dem neusten Stand, und ist die Performance ausreichend gewährleistet?



- Sind meine Mitarbeitenden genügend geschult, und verfügen sie über die richtigen Fähigkeiten?

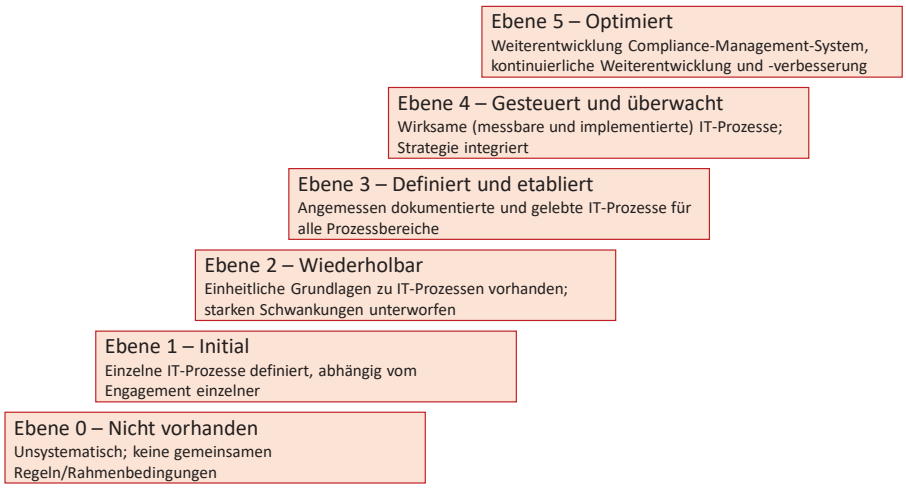
(siehe IT-Strategie und Vision)

OBT unterstützt Sie gerne bei einer ersten Beurteilung Ihrer IT-Umgebung und gibt Ihnen im Rahmen des IT-Health-Checks pragmatische und lösungsorientierte Empfehlungen, wie Sie Ihre IT-Prozesse mit wenigen, aber wirkungsvollen Anpassungen verbessern und IT-Risiken reduzieren können. In Gesprächen und in einem gemeinschaftlichen Ansatz diskutieren wir über Good/Best-Practice-Lösungen; dies zielgerichtet und auf Basis unserer Erfahrungen bei der Optimierung der Geschäfts- und IT-Prozesse, sowie der Reduzierung von IT-Risiken.

Unser Vorgehen ist transparent, startet mit einem Erstgespräch und einer Aufnahme der Selbsteinschätzung. Für diese erheben wir die Ist-Zustände im Bereich der generellen IT-Umgebung, um die drei Hauptebenen zu beurteilen. Auffälligkeiten werden offen diskutiert und können dadurch vertiefter geprüft und beurteilt werden.

Beurteilung der Kern-IT-Prozesse

Eine weiter gehende, vertiefte IT-Prüfung im Sinne einer Standortbestimmung hilft vielen Unternehmen, ihr Verbesserungspotenzial sowie «blinde Flecken» zu identifizieren. Diese Prüfung kann auf einem IT-Health-Check aufbauend vorgenommen werden. Die Beurteilung der IT-Umgebung bietet gleich mehrere Vorteile.



So lassen sich Lücken in den Bereichen Zugriffsberechtigungen, Änderungsmanagement, Programmentwicklung und IT-Betrieb mit relativ geringem Aufwand anhand von Befragungen und Stichproben mit den gemeinsam identifizierten Verantwortlichen aufdecken und verbessern. Zudem können Auffälligkeiten objektiv an einem Reifegradmodell gemessen und mit Unternehmen ähnlicher Grösse und Branche verglichen werden.

FAZIT

Die Welt unterliegt einem stetigen Wandel und bietet mit den Herausforderungen der Digitalisierung und Fragen zur IT-Sicherheit immer wieder Verbesserungspotenzial, um den IT-Risiken rechtzeitig und zweckmässig zu begegnen. Ein IT-Health-Check oder eine vertiefte IT-Prüfung bzw. projektbegleitende Prüfungen, z.B. im Rahmen einer Datenmigration oder einer Evaluierung des IT-IKS-Reifegrades, helfen dabei. OBT bietet verschiedene Produkte zur Unterstützung an und begleitet Sie mit pragmatischen und einfachen Lösungen.