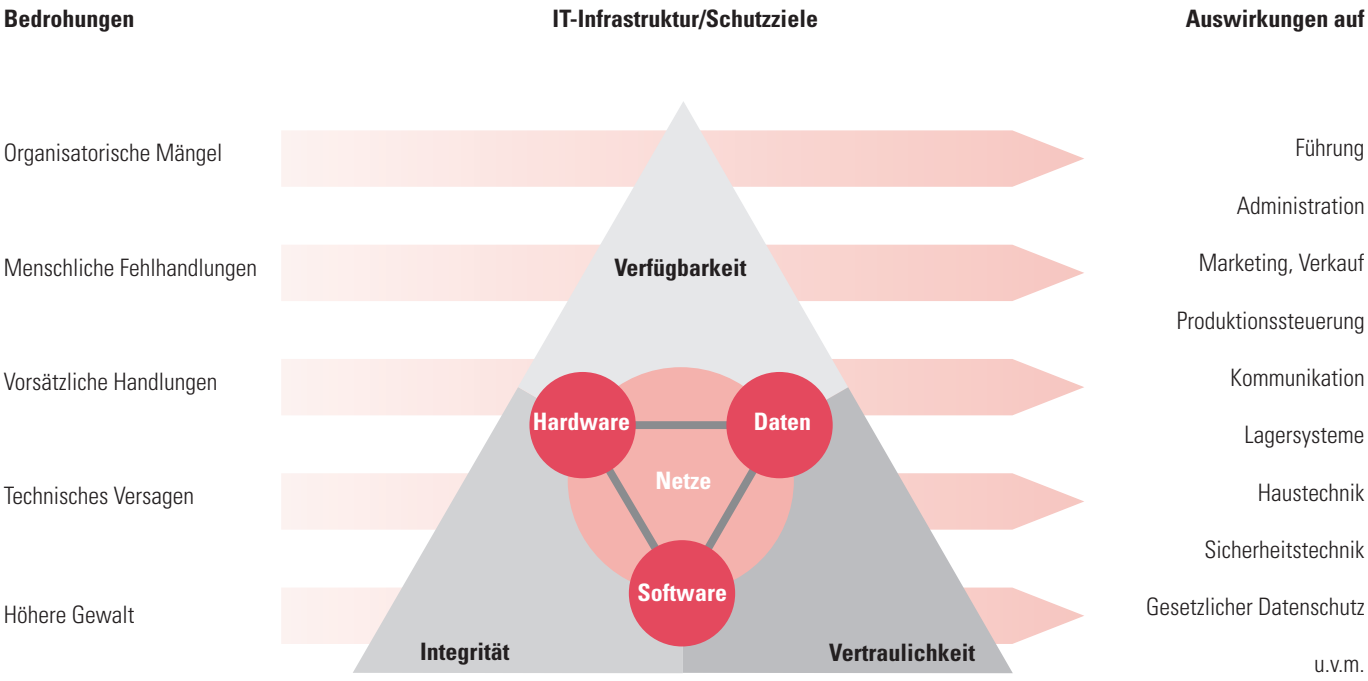
Wie viel IT-Sicherheit braucht Ihr Unternehmen?



Unerkannte Abhängigkeiten verursachen unzureichenden Schutz

Wie abhängig ist Ihr Unternehmen von IT-Systemen?

Die Benutzung von IT-Systemen im betrieblichen Alltag eines Unternehmens ist heute eine Selbstverständlichkeit. Neben der schnellen Abwicklung von Aufträgen, der ökonomischen Lagerbewirtschaftung und des reibungslosen Funktionierens der Administration steuern IT-Systeme vielfach auch Produktions-, haustechnische (Telefon-, Klima- und Heizungsanlagen) sowie sicherheitstechnische Anlagen (Brandmelde- und Überwachungsanlagen). Leider ist das Bewusstsein über die eigene Abhängigkeit von IT-Systemen und die daraus resultierende Verletzlichkeit nicht ausreichend vorhanden.

Wie steht es mit Ihrer IT-Sicherheit?

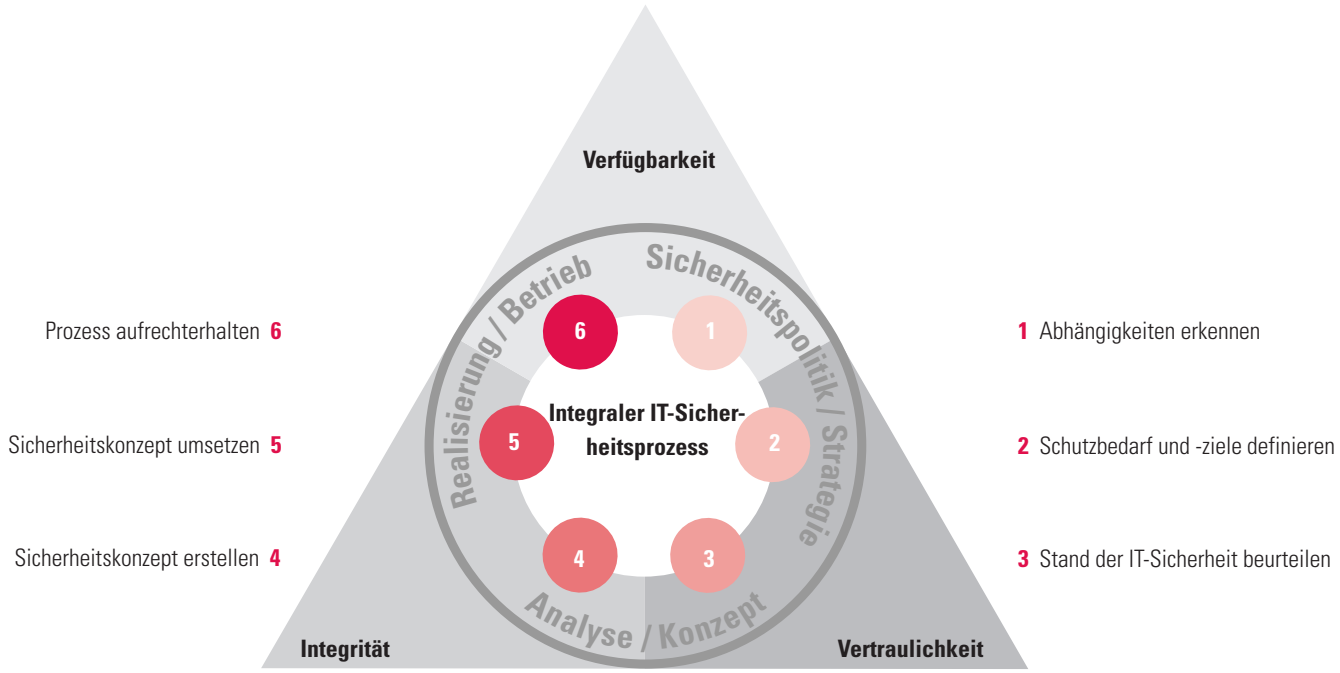
Die Gewährleistung der Verfügbarkeit von IT-Systemen, der Schutz der Vertraulichkeit und der Integrität von IT-Daten ist auch für ein kleines Unternehmen lebensnotwendig. Meist mit punktuellen und unkoordinierten Sicherheitsmassnahmen versuchen viele Unternehmen, die eigene IT-Infrastruktur zu schützen. Da sie aber oft über ein beschränktes IT-Engagement, keine oder eine unzureichende IT- Sicherheitsstrategie und -organisation verfügen, laufen sie allzu oft den Problemen hinterher. Dies ist nicht nur kostspielig, sondern ist auch für die Gesamt-IT-Sicherheit abträglich. Der Aufbau einer für das Unternehmen wirksamen und nachhaltigen IT-Sicherheit benötigt neben einer klaren Sicherheitsstrategie, ein methodisches Vorgehen sowie einen integralen Lösungsansatz.

Könnte es sein, dass Sie etwas übersehen haben?

Der ganzheitliche Ansatz von Basler & Hofmann hilft Ihnen, den Stand Ihrer IT-Sicherheit zu beurteilen sowie die allfällig notwendigen Sicherheitsmassnahmen zu planen und wirtschaftlich zu realisieren.

Der integrale IT-Sicherheitsprozess von Basler & Hofmann

Ein guter Schutz wird nur über einen systematischen und integralen IT-Sicherheitsprozess erreicht. Basler & Hofmann bietet Ihnen ein strukturiertes und modular aufgebautes Vorgehen an. Dieses stützt sich auf die ISO-Normen 17799 «IT-Code of practice for information security management» sowie das «IT-Grundschutzhandbuch» des Bundesamts für Sicherheit in der Informatiktechnik (D).



1

Abhängigkeiten des Unternehmens von der IT-Infrastruktur erkennen
Für die Festlegung des notwendigen IT-Schutzes sowie der anzustrebenden Schutzziele werden alle die für den Unternehmenserfolg kritischen Betriebsabläufe auf ihre Abhängigkeit von der eingesetzten IT-Infrastruktur überprüft. Eine vollständige Übersicht der bearbeiteten IT-Daten und eingesetzten IT-Systeme wird erarbeitet.

2

Schutzbedarf und -ziele definieren
Unter Einbezug der im Störfall entstehenden IT-Beeinträchtigung bzw. Schäden werden die Schutzziele bzw. der Schutzbedarf bezüglich der Verfügbarkeit, Integrität und Vertraulichkeit der erfassten IT-Daten und -Systeme sowie die notwendigen IT-Sicherheitsorganisation und Grundmassnahmen in einer IT-Policy schriftlich festgelegt. Die IT-Policy dient als Grundlage für die Erarbeitung eines IT-Sicherheitskonzeptes.

3

Stand der IT-Sicherheit beurteilen
Die systematische Erkennung eventueller Lücken in der bestehenden IT-Sicherheit hilft, Schwachstellen zu erfassen. Die organisatorischen, baulichen, technischen, personellen und rechtlichen Aspekte der IT-Sicherheit werden in einer Sicherheitsanalyse überprüft.

4

Sicherheitskonzept erstellen
Für die Bestimmung und Priotitätensetzung der notwendigen Sicherheitsmassnahmen werden der im Unternehmen festgelegte Schutzbedarf und der tatsächliche Stand der IT-Sicherheit miteinander verglichen. Ein dem Unternehmen angepasstes IT-Sicherheitskonzept, inklusive Realisierungsplan für die vereinbarten IT-Sicherheitsmassnahmen, wird unter Einbezug des Kunden erstellt.

5

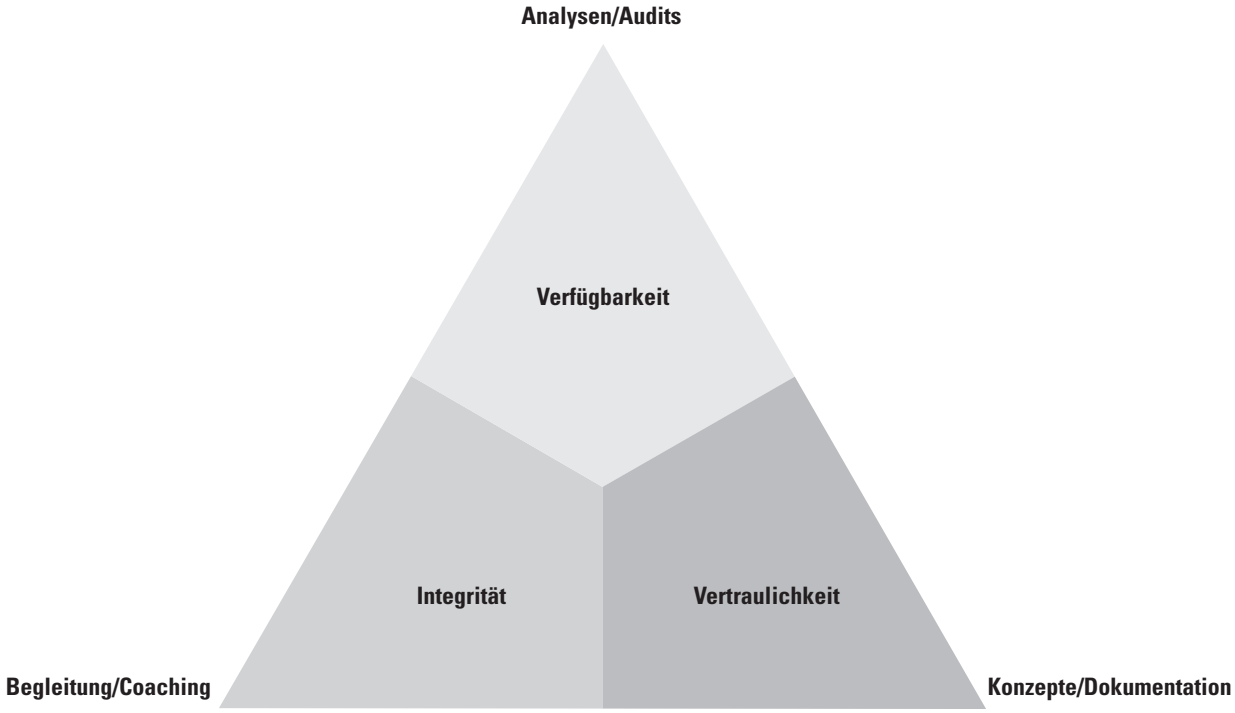
Sicherheitskonzept umsetzen
Systematische und koordinierte Umsetzung der im Sicherheitskonzept vereinbarten Massnahmen. Zur Förderung des IT-Sicherheitsbewusstseins wird für alle Ebenen der Organisation ein Schulungs- und Sensibilisierungsprogramm festgelegt.

6

Prozess aufrechterhalten
Die periodische Überprüfung der Sicherheitsmassnahmen auf ihre Funktion, die Beseitigung neu erkannter Schwachstellen sowie die Anpassung des Sicherheitskonzeptes an neue organisatorische, personelle, technische und rechtliche Gegebenheiten werden gewährleistet. So wird ein nachhaltiger IT-Schutz sichergestellt. Ein Reportingsystem wird eingeführt.

Unser Dienstleistungsangebot

Mit einem gezielten, lösungsorientierten Dienstleistungsangebot räumen wir für Sie die Hindernisse aus dem Weg.



Analysen/Audits

Basissicherheitsanalyse mit bewährtem Verfahren (siehe Rückseite)
- Erstüberprüfung des IT-Sicherheits-Standes (Ferndiagnose mit Checkliste)
- Empfindlichkeitsanalyse des bestehenden IT-Systems
- Massnahmenkatalog

Detailanalyse
- Physische Sicherheit (Brandschutz, Zutritt etc.)
- Logische Sicherheit (Datensicherung, Virenschutz, Internet etc.)
- Erfüllung der gesetzlichen Vorgaben

Prüfung der Netzwerk-Infrastruktur auf Schwachstellen
Prüfung der Performance von Netzwerken
Technologie- und Kompatibilitätsstudien

Konzepte/Dokumentation

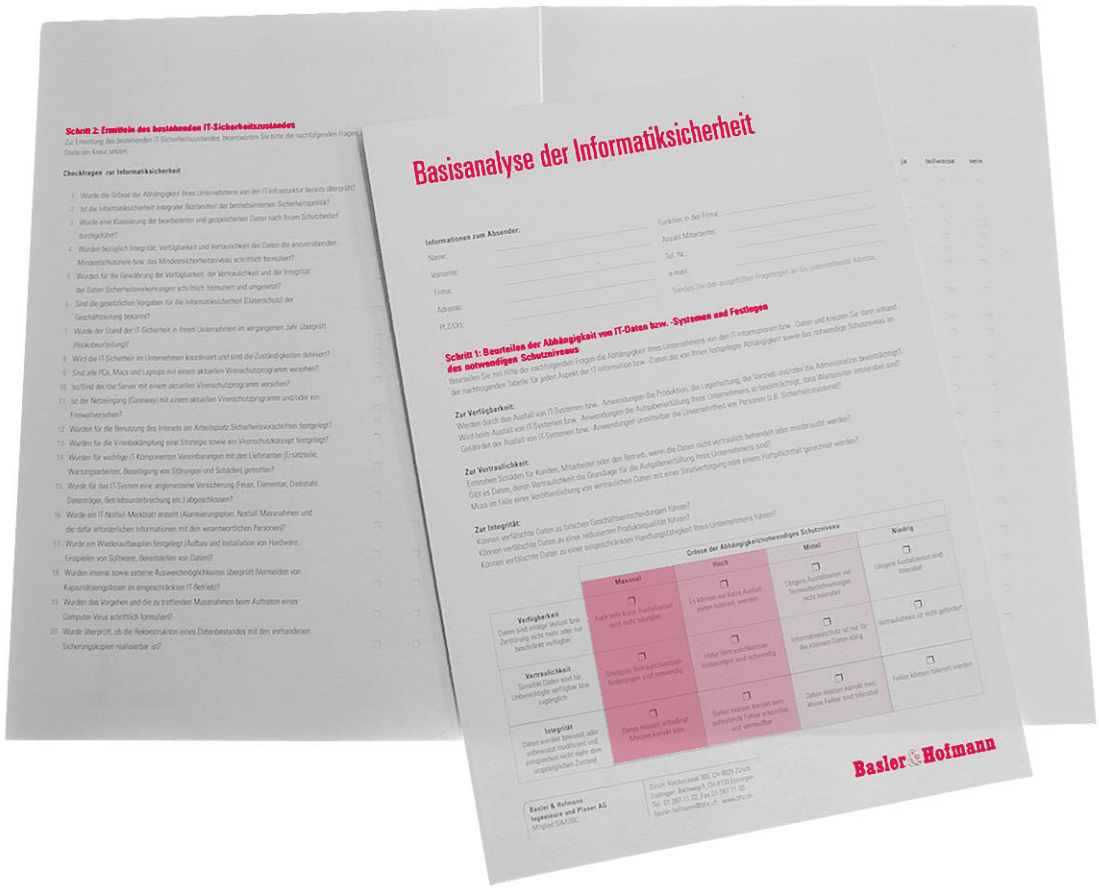
Erarbeiten von IT-Sicherheitskonzepten
- Physische Sicherheit (Brandschutz, Zutritt etc.)
- Logische Sicherheit (Datensicherung, Virenschutz, Internet etc.)

Erarbeiten von IT-Sicherheitsrichtlinien
Konzeptionelle Planung und Gestaltung von Netzwerk-Projekten

Begleitung/Coaching

Nach Bedarf unterstützen wir Sie bei folgenden Aufgaben
- Abhängigkeitsanalyse von IT-Systemen
- Festlegen des Schutzbedarfes (Verfügbarkeit, Vertraulichkeit und Integrität) und der Schutzziele
- Umsetzen der notwendigen IT-Sicherheitsmassnahmen
- Aufbau einer betriebsinternen IT-Sicherheitsorganisation
- Information, Sensibilisierung und Schulung der Mitarbeiterinnen und Mitarbeiter zu Themen der IT-Sicherheit

Projektplanung, Controlling und Qualitätssicherung von Informatikprojekten
Regelmässige Überwachungen und Revisionen der Netzwerkinstallationen
Pflege und Wartung von Netzwerken



Die Basisanalyse der IT-Sicherheit wird anhand einer standardisierten Checkliste durchgeführt und dient als erste kostengünstige Überprüfung des Ist-Zustandes der IT-Sicherheit. Dank dieser Analyse ist es möglich, gezielte Massnahmen zur Ergänzung der bestehenden IT-Sicherheit festzulegen und umzusetzen.

Zusätzliche Informationen zur Basisanalyse sowie allen weiteren Dienstleistungen von Basler & Hofmann erhalten Sie unter www.bhz.ch.