# Netzwerk- und Informationssicherheit




## Zielsetzung

Schaden von Netzwerkinfrastrukturen und deren Anwendungen abzuwenden sowie der Schutz von Informationen, ist Ziel des IP Systems Angebots. Wir richten uns mit unserem Unterstützungsangebot an IT-Sicherheitsverantwortliche und Sicherheitsexperten.

Wir unterstützen Sie bei der Planung und der Umsetzung von Maßnahmen zum Schutz ihrer ITK-Infrastruktur. Dazu betrachten wir insbesondere die Aspekte Vertraulichkeit, Integrität und Verfügbarkeit sowie prozessorientierte, organisatorische und technologische Fragestellungen:

- Prozessorientiert zum Herstellen reibungsarmer Abläufe
- Organisatorisch zum Einbetten in die Unternehmensstrategie
- Technologisch, um Aspekte, wie z.B. Systemkomponenten, Inventar, Daten und Standards wie ISO und BSI Vorschriften ebenfalls mit einzubeziehen.

IT-Sicherheit ist für uns der wirksame Schutz Ihrer Unternehmensressourcen mit beherrschbaren Risiken, verbunden mit Absicherungen gegen unerwünschte Einwirkungen von innen (Organisation) und außen (Internet) oder andere Fremdzugänge. Ein punktueller Ansatz genügt hier nicht, ein Ende-zu-Ende-Systemansatz ist notwendig.

## Motivation

Die Bedeutung der Sicherheit in der Informations- und Telekommunikationstechnik (ITK) in Industrie und öffentlicher Verwaltung ist gestiegen. Insbesondere gilt das für den Bereich von kritischen Infrastrukturen. Die Bedeutung des Schutzes und der Sicherheit wird durch das im Jahre 2015 in Kraft getretene IT-Sicherheitsgesetz hervorgehoben.
Betroffen sind Unternehmen und Verwaltungen, die ITK-Infrastrukturen betreiben und entsprechende Dienste für Sprache und Daten, inklusive des Vorhaltens von Daten, erbringen. Mögliche Informationsabflüsse oder das Manipulieren von Daten können beträchtliche Schäden anrichten und die Arbeitsfähigkeit bzw. Versorgung von Dienstleistungen temporär stilllegen.
Auf Grund der zunehmenden Fortentwicklung der ITK, der geplanten Digitalisierung (z.B. IoT) bzw. Automatisierung entstehen erhöhte Angriffs- und Bedrohungspotentiale. Diesen gilt es zu begegnen und Risiken zu minimieren.

## Unsere Leistungen:

- Analyse (Ende-zu-Ende)
- Ist-Abgleich
- Aufzeigen von Schwachstellen und Risiken
- Design und Konzeption
- Implementierung
- Administration und Betrieb
- Fortschreibung und Dokumentation

mit folgenden Ergebnissen:

- Identifizieren von Schwachstellen
- Aufzeigen von Schutzmaßnahmen (z.B. Kryptographie)
- Konzeption und Umsetzen der Schutzmaßnahmen
- Verifikation und Test der Wirksamkeit der Maßnahmen
- Schutz der ITK-Infrastruktur (OSI Layer)
- Sichere Kommunikation von „innen“ und „außen“
- Verbesserter Betrieb der IT-Infrastruktur
- IT-Managementsystem

## Vorgehensweise

Wir verstehen das Thema Netzwerk- und Informationssicherheit als einen kontinuierlichen Prozess. Dies wird in Abbildung 1 verdeutlicht:

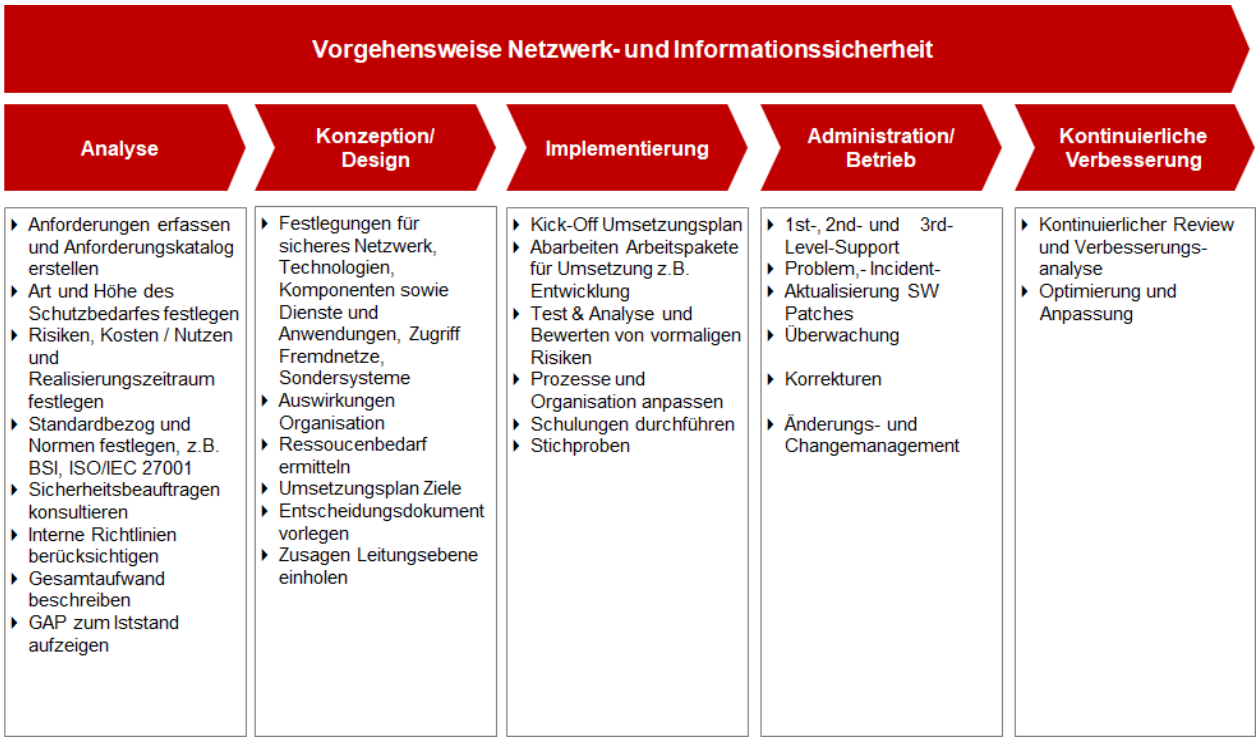


*Abbildung 1*

Zu Beginn wird eine Anforderungsanalyse mit resultierender Schutzbedarfsfeststellung durchgeführt, in der, ausgehend von identifizierten Risiken und Gefährdungen, die Art und Höhe des Schutzbedarfes festgelegt wird. Ggf. werden auch Penetrationstests (PEN-Tests) durchgeführt, die noch unbekannte Schwachstellen in der bestehenden Sicherheitsarchitektur aufdecken. Wir betrachten betroffene Komponenten, Dienste und Anwendungen sowie die Organisation mit Ihren Prozessen als Ganzes.

Wir orientieren uns an relevanten Festlegungen des BSI für kritische Infrastrukturen (KRITIS) sowie Normen und Standards, wie z.B. DIN ISO/IEC 27001. Für Infrastrukturen mit niedrigeren Sicherheitsbedürfnissen finden wir adäquate industrietypische Lösungen.

Die Analysephase betrachtet die festgelegten Anforderungen zum Schutzbedarf und mündet in einer Gap-Analyse zum avisierten Ziel. In Zusammenarbeit mit den IT-Verantwortlichen wird diese erstellt und abgestimmt. Die Ergebnisse bilden die Grundlage für das Konzept und die spätere Implementierung.

Die Konzeption beinhaltet entsprechende Maßnahmen, die dazu führen, Festlegungen für eine sichere Netzwerkarchitektur zu treffen. Wesentlich ist hier die Akzeptanz der Leitungsebene zu den vorgeschlagenen Maßnahmen, die abgestimmt in die Umsetzungphase münden. Auf dieser Basis wird sichergestellt, dass die festgelegten Ziele implementierbar sind. Die Entscheidungsvorlage und anschließende Genehmigung schließen diese Phase ab.

Nach der Freigabe der Leitungsebene zu den entsprechenden Schutzmaßnahmen und erforderlichen Ressoucen, wird die Implementierung begonnen. Arbeitspakete werden schrittweise umgesetzt und bei Änderungen im Dialog entsprechend angepasst. Test und Analyse zur Konformität und Feststellen der Funktionsweise in der angepassten Infrastruktur sichern die Zielumsetzung ab. In der Implementierung wird ebenfalls überprüft, ob vormalige Risiken mit den getroffenen Maßnahmen gemildert bzw. geschlossen wurden.

Der Faktor Mensch stellt beim Thema Sicherheit eine entscheidende Größe dar, da die Sicherheitsmaßnahmen immer mit einer Umsetzung durch die Mitarbeiter einhergehen. Daher ist zu beachten, dass die Sensibilisierung und Umsetzungstreue auf verschiedenen Ebenen der Mitarbeiter für die gemeinsame Zielsetzung im Bereich Sicherheit erfolgskritisch und unabdingbar ist. Entsprechende Schulungen und regelmäßige Stichproben zur Prozesskonformität sichern den Erfolg ab.

In der Administrations- und Betriebsphase werden die eingeführten Maßnahmen kontinuierlich auf ihre Wirkung hin überwacht und erforderlichenfalls Korrekturmaßnahmen eigeleitet. Dies erfolgt auf Basis festgeschriebener standardisierter Prozesse im Rahmen eines kontinuierlichen Verbesserungsprozesses (KVP).

Der KVP bedingt auch eine Implementierung im Unternehmen – hier ist ein Top-Down-Ansatz von der Leitungsebene erforderlich. Die Aufgabe im Betrieb besteht sowohl darin, proaktive Maßnahmen gegen mögliche Angriffs- und Gefahrenpotenziale frühzeitig zu erkennen, in geordneter Weise auf mögliche Sicherheitsvorfälle zu reagieren und evt. erforderliche Maßnahmen wie z.B. Umplanungen durchzuführen.

Wir empfehlen eine Zuordnung auf Basis des OSI Modells hinsichtlich der Schutzkriterien vornehmen. Dies wird im nachfolgenden Schaubild 2 verdeutlicht.

Die ISO/OSI Schichten in 2 Bereichen zusammengefasst:

- Ebene 1: Anwendungen, Dienste und Endgeräte
- Ebene 2: Netzwerk und Komponenten

Dies vereinfacht die anschließende Zuordnung der verschiedenen Schutzkriterien als Zielsetzung für die weitergehende Analyse und des zu entwickelnden Sicherheitsdesigns im Rahmen des zuvor vorgestellten Vorgehensmodells.

Auf Grundlage unserer strukturierten Arbeit und Vorgehensweise ist IP Systems in der Lage, die gemeinsam entwickelten Ziele adäquat und qualitativ hochwertig umzusetzen.

Wir freuen uns, Sie bei Ihren Zielstellungen unterstützen zu dürfen.

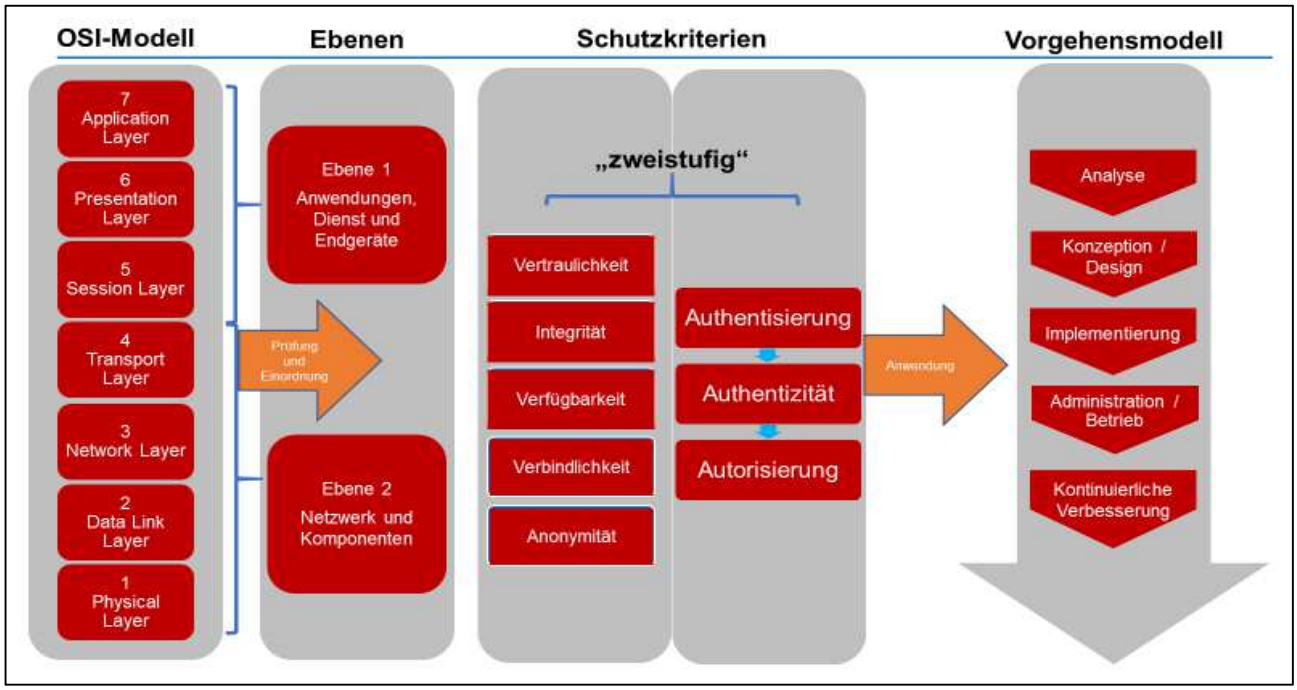


*Abbildung 2*