

IT-Sicherheit im Überblick

Die Sicherheit von Informationen ist enorm wichtig, nicht nur im privaten Bereich, sondern vor allem auch in der Wirtschaft. Im Rahmen der Informationssicherheit sind drei grundlegende Aspekte zu beachten:

- **Vertraulichkeit** als Schutz gegen unbefugte Informationsbeschaffung
- **Integrität** als Schutz gegen unbefugte Manipulation von Informationen
- **Verfügbarkeit** als Schutz gegen die Beeinträchtigung der Funktionalität des Systems

Die IT-Sicherheit ist ein Teil der Informationssicherheit, die sich auf elektronisch gespeicherte Daten und Informationen bezieht. Die IT-Sicherheit hat damit eine Schlüsselrolle in der digitalisierten Welt. Vertraulichkeit, Integrität und Verfügbarkeit sind dabei vielfältigen Bedrohungen ausgesetzt, vom Virus bis hin zu professionell angelegtem Abhören von Datenleitungen oder auch Täuschungsmanövern über manipulierte Internetseiten. Aber auch das unbefugte Lesen von Dokumenten von Mitarbeitern muss entsprechend verhindert werden (beispielsweise durch elektronische Zugangskontrollen).

Die geplante Vorgehensweise, um IT-Sicherheit zu gewährleisten ist der Aufbau eines IT-Sicherheitsmanagementsystems. Dazu kann vor allem die **ISO/IEC-Norm 27000** sowie deren Nachfolger dienen. Diese Norm beschreibt den Aufbau eines ISMS (Informationssicherheitsmanagementsystem). Alternativ bietet das *Bundesamt für Sicherheit in der Informationstechnik (BSI)* einen Leitfaden zum Aufbau eines IT-Sicherheitsmanagementsystems in Form des **IT-Grundschatzes**. Der IT-Grundschatz ist aber eng an die ISO/IEC-Norm 27000 angelehnt und dient auch als Basis für eine mögliche Zertifizierung für diese Norm.

Neben diesen Normen und Standards zur IT-Sicherheit wurde bereits 2015 ein Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) eingeführt und soll dazu dienen, die IT-Systeme und digitalen Infrastrukturen Deutschlands zu den sichersten weltweit zu machen. Dazu gehören vor allem die Bereiche der Kritischen Infrastrukturen (**KRITIS**), wie beispielsweise die Strom- und Wasserversorgung.

Ergänzt wird das Gesetz durch eine Partnerschaft von Staat und Wirtschaft mit dem Ziel, die Dienstleistungen kritischer Infrastrukturen aufrecht zu erhalten und zu schützen. Diese Partnerschaft begann schon im Jahr 2007 und hat auch maßgeblich zu Gestaltung des IT-Sicherheitsgesetzes beigetragen. Die Partnerschaft hieß zu Beginn **Umsetzungsplan kritischer Infrastrukturen** (UP KRITIS) und wird unter diesem Eigennamen **UP KRITIS** nun fortgeführt.

2.4.3 IT-Grundschutz

Ausgangsszenario:

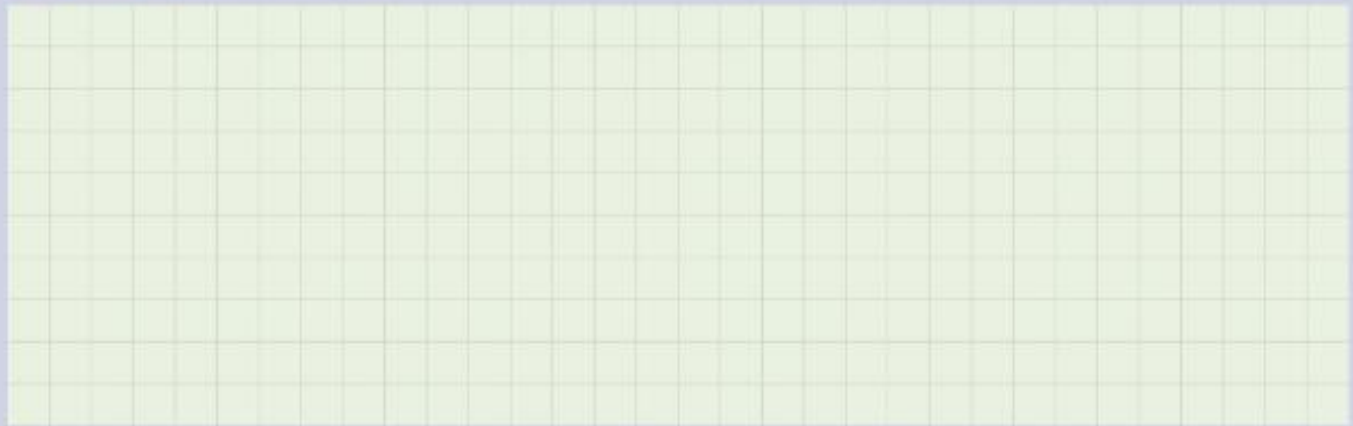
Die Geschäftsleitung der IT-Firma *ConSystem GmbH* möchte das Wissen über den IT-Grundschutz in der Firma erhöhen. Neben einigen Schulungen zu dem Thema soll auch ein kleiner Test überprüfen, ob die Mitarbeiter ihr Wissen erhöht haben.

Aufgabenstellung:

Der Leiter der Abteilung Entwicklung hat einen kleinen Test zu diesem Thema erstellt. Als erfahrener Auszubildender der Firma erhalten Sie den Auftrag eine Musterlösung zu diesem Test zu erstellen.

Test zu Thema IT-Grundschutz

Aufgabe 1: Was ist das BSI?



Aufgabe 2: Was versteht man unter IT-Grundschutz?



Aufgabe 3: Was ist eine Sicherheitsleitlinie im Vergleich zu einem Sicherheitskonzept?



Aufgabe 4: Im Rahmen des IT-Grundschutzes wird ein Sicherheitskonzept (Standard-Absicherung) vom BSI vorgeschlagen. Tragen Sie die Schritte dieser Absicherung in der korrekten Reihenfolge in das Diagramm ein.



Schritte:

- Auswahl der Sicherheitsanforderungen
- Analyse des IT-Zustandes
- Realisierung der Maßnahmen
- Aufrechterhaltung und kontinuierliche Verbesserung
- Schutzbedarfsfeststellung

Aufgabe 4: Welche Aufgaben hat ein Informationssicherheitsbeauftragter?

- ☐ Konfiguration der Sicherheitstechnik in der Firma
- ☐ Koordination der Entwicklung eines Sicherheitskonzeptes
- ☐ Berichte an die Geschäftsleitung über den aktuellen Stand der Informationssicherheit
- ☐ Fragen der Presse oder interessierter Bürger zum Stand der Informationssicherheit beantworten
- ☐ Leitung des Einkaufs der Software zur Abwehr von Schadprogrammen

2.4.4 Schutzbedarfsfeststellung

Ausgangsszenario:

Die Geschäftsleitung der IT-Firma **ConSystem GmbH** hat alle Abteilungen beauftragt eine Schutzbedarfsfeststellung im Rahmen der Umsetzung des IT-Grundschatzes durchzuführen.

Aufgabenstellung:

Der Leiter der Abteilung Entwicklung hat bereits wesentliche Aspekte für seine Abteilung zusammengetragen. Er bittet Sie als erfahrenen Auszubildenden der Firma diese Zusammenstellung zu einer aussagekräftigen Schutzbedarfsfeststellung zu vervollständigen. Dazu gehört auch, wichtige Begriffe zu definieren, damit die Mitarbeiterinnen und Mitarbeiter der Abteilung die Feststellung besser verstehen können.

Schutzbedarfsfeststellung Abteilung Entwicklung

Begriffsdefinitionen:

Vertraulichkeit:

Integrität:

Verfügbarkeit:

Schutzbedarfe:

System	Schutzziel mit Schutzbedarf	Begründung
Entwickler-PC mit Software zur Anwendungsentwicklung	Vertraulichkeit:	
	Integrität:	
	Verfügbarkeit:	
Internet-Router	Vertraulichkeit:	
	Integrität:	
	Verfügbarkeit:	

Hinweis: Kategorien des Schutzbedarfes

normal: Die Schadensauswirkungen sind begrenzt und überschaubar.

hoch: Die Schadensauswirkungen können beträchtlich sein.

sehr hoch: Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.

2.4.5 IT-Sicherheitsgesetz

Ausgangsszenario:

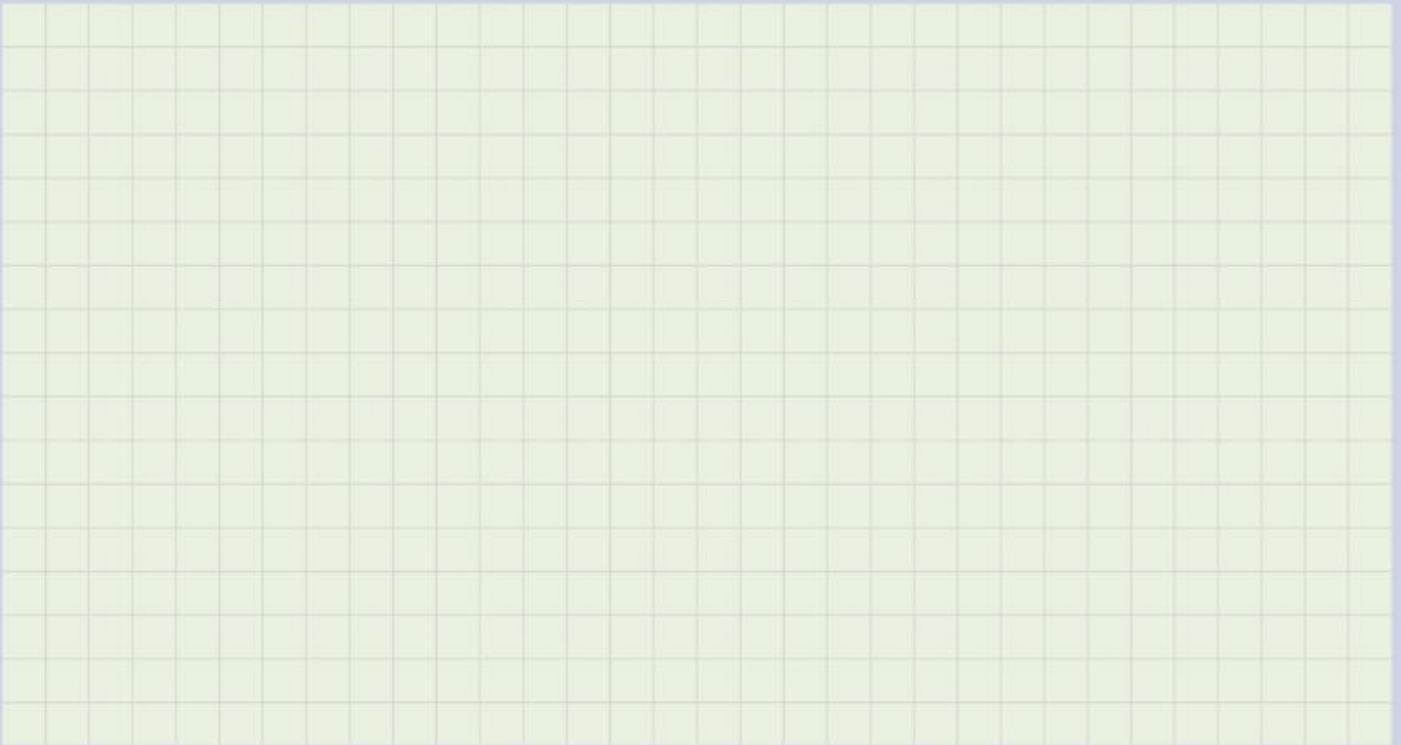
Die Geschäftsleitung der IT-Firma **ConSystem GmbH** möchte Kunden gewinnen, die nach dem IT-Sicherheitsgesetz (gültig seit Juli 2015) zur **kritischen Infrastruktur** gehören. Dazu wird die Entwicklungsabteilung beauftragt, wesentliche Informationen bereitzustellen.

Aufgabenstellung:

Der Leiter der Abteilung Entwicklung hat bereits Informationen zum IT-Sicherheitsgesetz zusammengetragen. Als erfahrener Auszubildender der Firma erhalten Sie den Auftrag diese Informationen zu vervollständigen.

Informationen zum IT-Sicherheitsgesetz

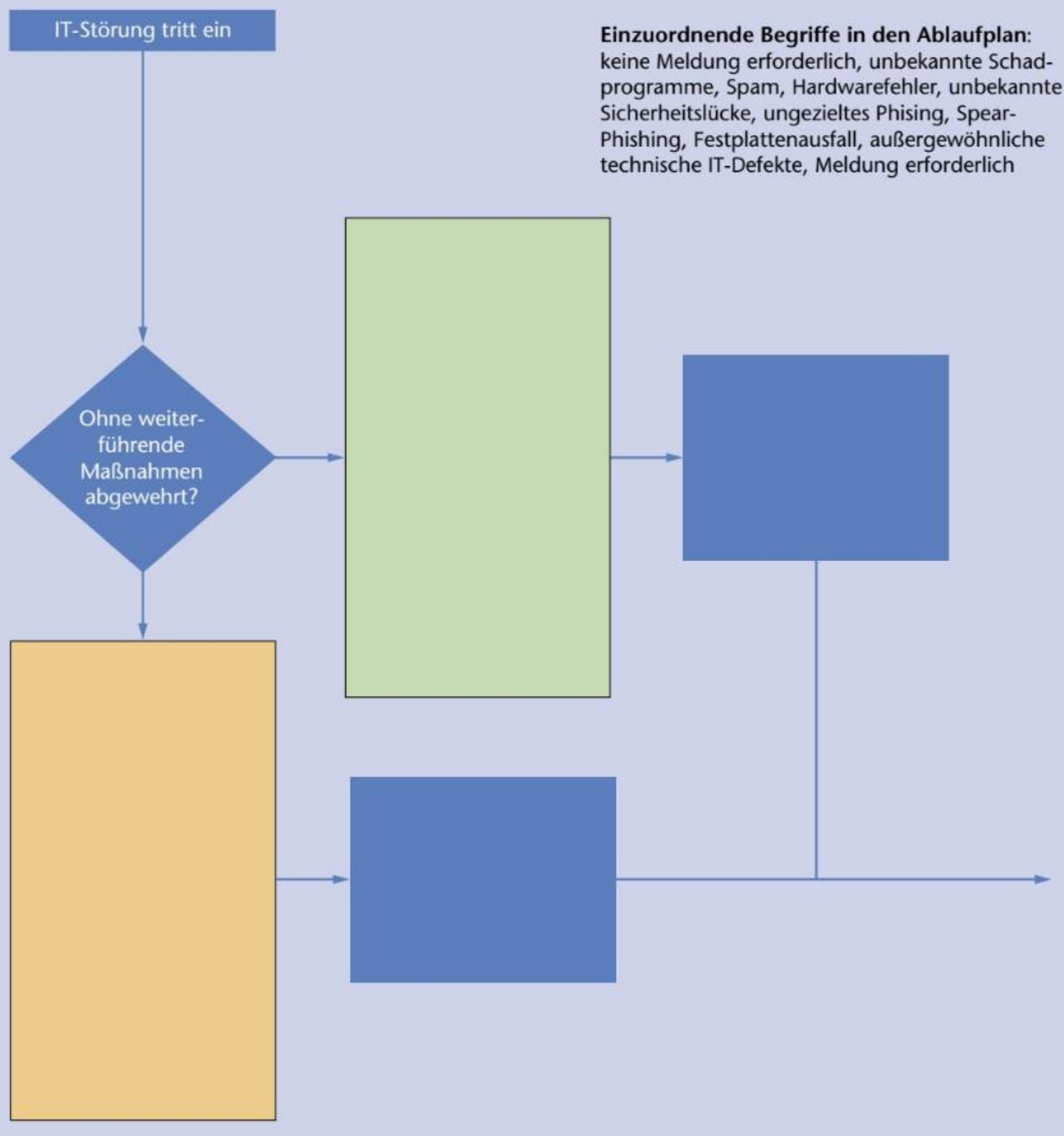
Kurzbeschreibung des IT-Sicherheitsgesetzes:



Sektoren der kritischen Infrastruktur:



Ablaufplan der Meldung einer IT-Störung:



2.4.6 Überblick IT-Sicherheit

Ausgangsszenario:

Die IT-Firma **ConSystem GmbH** möchte die Consulting-Dienstleistungen auch verstärkt im Bereich der IT-Sicherheit anbieten. Das schließt auch die Hilfe bei der Einführung eines Informationssicherheitsmanagementsystems sein. Die Geschäftsleitung der Firma hat beschlossen, dass die Kenntnisse der entsprechenden Mitarbeiter in diesem Bereich verbessert werden sollten.

Aufgabenstellung:

Der Leiter der Abteilung Entwicklung hat dazu verschiedene Begriffe zu diesem Bereich recherchiert und versucht, sie in einer Mindmap zu strukturieren. Als Auszubildender der Abteilung bittet er Sie, die Mindmap fertigzustellen.

Internetrecherche zur IT-Sicherheit

Begriffe:

Informationssicherheitsmanagementsystem	DIN ISO / IEC 27001	BSI
Gesetze	Schutzbedarfsfeststellung	DSG00 / BDSG
Auftragsdatenverarbeitung	IT-Grundschutz	KRITIS
Sicherheitskonzept	IT-Sicherheitsgesetz	
Industrielle Steuerungs- und Automatisierungssysteme (ICS)-Security		

Mindmap:

