IT-Security

> IT-Sicherheit reicht vom Schutz einzelner Dateien bis hin zur Absicherung von Rechenzentren und Cloud-Diensten. IT-Security gehört zu jeder Planung und Maßnahme in der IT und ist grundlegend für die Compliance im Unternehmen.

Unter IT-Sicherheit versteht man alle Planungen, Maßnahmen und Kontrollen, die dem Schutz der IT dienen. Der Schutz der IT hat drei klassische Ziele: **Die Vertraulichkeit der Informationen, die Integrität der Informationen und Systeme und die Verfügbarkeit der Informationen und Systeme**. Der Schutz der IT-Systeme vor Ausfall und die notwendige Belastbarkeit der IT-Systeme ist grundlegend für die Aufrechterhaltung des Geschäftsbetriebs, für die „Business Continuity“.

Im Gegensatz zur Datensicherheit geht es in der IT-Sicherheit nicht nur um personenbezogene Daten, für die der rechtlich geforderte Datenschutz Sicherheitsmaßnahmen verlangt. Es geht vielmehr um alle Arten von Informationen, die es zu schützen gilt.

Informationssicherheit

In der Informationssicherheit geht es allgemein um den Schutz von Informationen. Diese können auch in nicht-technischen Systemen vorliegen, zum Beispiel auf Papier. Die Schutzziele der Informationssicherheit bestehen darin, die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sicherzustellen.
In Deutschland gilt der IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI) als Leitlinie für die Informationssicherheit.

Im Anhang A der **ISO 27001** gibt es eine Liste von 114 Sicherheitsmaßnahmen zur Überprüfung des Sicherheitsniveaus in Unternehmen, sogenannte Controls. Zum Schutz des geistigen Eigentums können wir diese hier nicht einfach auflisten. Die 14 Abschnitte des Anhang A mit kurzer Erklärung:

- **A.5 Informationssicherheitspolitik** – Kontrollen, wie die Politik geschrieben und überprüft ist
- **A.6 Organisation der Informationssicherheit** – Kontrollen, wie die Verantwortlichkeiten zugewiesen sind, enthält auch die Kontrollen für Mobilgeräte und Telearbeit
- **A.7 Personalsicherheit** – Kontrollen vor, während und nach der Anstellung
- **A.8 Asset Management** – Kontrollen in Bezug auf das Asset-Verzeichnis und akzeptable Nutzung sowie auch für Informationsklassifizierung und Medien-Handhabung
- **A.9 Zugriffskontrolle** – Kontrollen für die Zugriffskontrollen-Richtlinie, die Benutzerzugriffsverwaltung, System- und Applikations-Zugriffskontrolle sowie

Anwenderverantwortlichkeiten
- **A.10 Kryptografie** – Kontrollen in Bezug auf Verschlüsselung und Schlüsselverwaltung
- **A.11 Physische und Umgebungssicherheit** – Kontrollen, die Sicherheitsbereiche, Zutrittskontrollen, Schutz gegen Bedrohungen, Gerätesicherheit, sichere Entsorgung, Clear Desk- und Clear Screen-Richtlinie usw. definieren
- **A.12 Betriebssicherheit** – eine Menge an Kontrollen im Zusammenhang mit dem Management der IT-Produktion: Change Management, Capacity Management, Malware, Backup, Protokollierung, Überwachung, Installation, Schwachstellen usw.
- **A.13 Kommunikationssicherheit** – Kontrollen in Bezug auf Netzwerksicherheit, Segregation, Netzwerk-Services, Informationstransfer, Nachrichtenübermittlung etc.
- **A.14 Systemerwerb, Entwicklung und Wartung** – Kontrollen, die Sicherheitsanforderungen und die Sicherheit in Entwicklungs- und Support-Prozessen definieren
- **A.15 Lieferantenbeziehungen** – Kontrollen, was in Vereinbarungen zu inkludieren ist und wie die Lieferanten zu überwachen sind
- **A.16 Informationssicherheits-Störfallmanagement** – Kontrollen für die Meldung von Vorfällen und Gebrechen, welche die Verantwortlichkeiten, Sofortmaßnahmen und Sammlung von Beweisen definieren
- **A.17 Informationssicherheitsaspekte des betrieblichen Kontinuitätsmanagements** – Kontrollen, welche die Planung von Betriebskontinuität, Verfahren, Verifizierung und Überprüfung sowie der IT-Redundanz verlangen
- **A.18 Compliance/Konformität** – Kontrollen, welche die Identifizierung anwendbarer Gesetze und Bestimmungen, des Schutzes geistigen Eigentums, des Schutzes persönlicher Daten und die Überprüfung der Informationssicherheit verlangen

Datensicherheit

Datensicherheit hat **das Ziel, die Vertraulichkeit, Integrität und Verfügbarkeit von Daten sicherzustellen**. Im Unterschied zum Datenschutz beschränkt sie sich nicht auf personenbezogene Daten, sondern erstreckt sich auf alle Daten. **Vertraulichkeit** bedeutet, dass nur befugte Personen auf die Daten zugreifen können. **Integrität** heißt: Die Daten wurden nicht manipuliert oder beschädigt. Die **Verfügbarkeit** bezieht sich darauf, dass Daten verwendet werden können, wenn man sie benötigt. Um Datensicherheit zu etablieren, sind verschiedene technische und organisatorische Maßnahmen nötig, zum Beispiel Zugriffskontrollen, Kryptografie oder redundante Speichersysteme.

Um Datensicherheit zu etablieren, sind verschiedene technische und organisatorische Maßnahmen nötig, zum Beispiel **Zugriffskontrollen**, **Kryptografie** oder **redundante Speichersysteme**.

Information Security Management System (ISMS)

Ein Informationssicherheits-Management-System, auf Englisch „Information Security Management System (ISMS)“, ist kein technisches System, sondern **definiert Regeln und Methoden, um die Informationssicherheit zu gewährleisten, zu überprüfen und kontinuierlich zu verbessern**. Das umfasst unter anderem die Ermittlung und Bewertung von Risiken, die Festlegung von Sicherheitszielen sowie eine klare Definition und Dokumentation von

Verantwortlichkeiten, Kommunikationswegen und Abläufen.

Cyber-Resilienz

Unter Cyber-Resilienz versteht man die Fähigkeit eines Unternehmens oder einer Organisation, ihre **Geschäftsprozesse trotz widriger Cyber-Umstände aufrechtzuerhalten**. Das können Cyber-Angriffe sein, aber auch unbeabsichtigte Hindernisse wie ein fehlgeschlagenes Software-Update oder menschliches Versagen. Cyber-Resilienz ist ein umfassendes Konzept, das über die IT-Sicherheit hinausgeht. Es vereint die Bereiche Informationssicherheit, Business-Kontinuität und organisatorische Resilienz. Um einen Zustand der Cyber-Resilienz zu erreichen, ist es wichtig, Schwachstellen frühzeitig zu erkennen, sie wirtschaftlich zu priorisieren und zu beseitigen.

Authentisierung, Authentifizierung und Autorisierung

Die **Authentisierung** stellt den Nachweis einer Person dar, dass sie tatsächlich diejenige Person ist, die sie vorgibt zu sein. Eine Person legt also Nachweise vor, die ihre Identität bestätigen sollen.

Die **Authentifizierung** stellt eine Prüfung der behaupteten Authentisierung dar. Bei der Authentifizierung ist nun der Prüfer an der Reihe. Er überprüft die Angaben auf ihre Echtheit. Zeitlich betrachtet findet eine „Authentifizierung“ also nach einer „Authentisierung“ statt.

Die **Autorisierung** ist die Einräumung von speziellen Rechten. War die Identifizierung einer Person erfolgreich, heißt es noch nicht automatisch, dass diese Person bereitgestellte Dienste und Leistungen nutzen darf. Darüber entscheidet die Autorisierung.

Schutzbedarfsstufen

normal	hoch	sehr hoch
Die Schadensauswirkungen sind begrenzt und überschaubar.	Die Schadensauswirkungen können beträchtlich sein.	Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.

Beispiele für Sicherheitstests / Penetrationstest / Eindringungstest / Juckts im Schritt?

- Überprüfung der vom Kunden zur Verfügung gestellten Daten auf Korrektheit
- Identifizierung von Betriebssystemen und erreichbaren Diensten
- Test der erkannten Dienste mit Schwachstellenscannern
- Überprüfung der Ergebnisse, Verifizierung von erkannten Sicherheitslücken
- Einsatz von Werkzeugen, die Gebiete abdecken, die von Schwachstellenscannern nicht berücksichtigt werden
- Manuelle Prüfungen
- Nachweis von DoS-Potenzialen nach Absprache mit dem Kunden

Created 2022-08-01 07:32:29 UTC by Joshua Lieder
Updated 2022-10-31 09:05:20 UTC