# Mobile Infrastrukturen
# Studiengang Informatik


- Dipl.-Inf., Dipl.-Ing. (FH)  Michael Wilhelm
- Hochschule Harz
- FB Automatisierung und Informatik
- mwilhelm@hs-harz.de
- Raum 2.202
- Tel. 03943 / 659 338




## Inhalt

- **Rechnerstrukturen ohne Tablets (Hardware / Software)**
  - Ebenen der IT-Infrastruktur
  - Rechenzentrum (Desktop-Rechner)
- **Erweiterung auf „Mobile Infrastrukturen“**
  - Rechenzentrum + Mobile Infrastrukturen
- **Komponenten_mobiler_Infrastrukturen**
- **Gesetze**
- **Sicherheitsprobleme bei Smartphones und Tablets**
- **Mobile Device Management**

# Gesetzesgrundlagen

- **ISO 27000 / 27001 / 27002 / 27003 / 27004**
  - Definiert Standards für ein Integriertes Sicherheitsmanagentsystem (ISMS)
  - Wie kann man es zertifizieren?
  - Welche Prozesse sind notwendig?
  - Welches Personal benötigt man?
  - Welche Resourcen benötigt man? (Hardware, Software, Richtlinien…)
  - Viren / Co: E-Mail-Anhang (Ransomware …)
  - Diese Dokumentationen geben einen Rahmen (keine Details).
- **IT-Grundschutz vom BSI**
  - Insgesamt detaillierter als die ISO 2700x.
  - Bezieht sich auf die allgemeine Sicherheit (ohne mobile Infrastruktur).
  - Informationssicherheit_mit_System.pdf (Überblick).
  - IT_Grundschutz_Kompendium_Edition2022.pdf (900 Seiten).

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html



# Die BSI-Standards

- Aufbau und Etablierung eines ISMS.
- drei Vorgehensweisen für unterschiedliche Anwendungsfälle.
- abgestimmt auf das IT-Grundschutz-Kompendium.
- umfassen auch Risikomanagement und Notfallmanagement.
- ISO/IEC 27001- bzw. ISO/IEC 22301-kompatibel.
- ISO 27001-Zertifizierung auf Basis von IT-Grundschutz möglich.

## IT Grundschutz (Allgemein)

- **Elementare Gefährdungen (Auswahl):**
  - Feuer / Wasser / Verschmutzung etc.
  - Ausfall der Stromversorgungen / Dienstleistungen, Netze
  - Abhören
  - Diebstahl, Verlust von Geräten, Zerstören von Geräten
  - Manipulation von Informationen
  - Unbefugtes Eindringen in IT-Systeme
  - Anschlag, Erpressung, Schadprogramme, Sabotage
  - Datenverlust
  - Personalausfall, Resourcenmangel
  - Software-Schachstellen oder Fehler
  - Unberechtigte Nutzung von Geräten und Systemen, Missbrauch von Berechtigungen
  - Verhinderung von Diensten (Denial of Service)



## IT Grundschutz (Allgemein)

- **Prozess-Bausteine (Auswahl):**
  - Sicherheitsmanagement
  - Organisation
  - Personal
  - Schulung
  - Kryptokonzept
  - Datenschutz
  - Informationssicherheit auf Auslandsreisen
  - Software-Entwicklung
  - Software-Entwicklung von Webanwendungen
  - Betrieb (Patch, Protokolle, Telearbeit, Fernwartung)
  - Cloud
  - Sicherheitsüberprüfungen (Vorgaben, Tests, Revisionen)

## IT Grundschutz (Allgemein)

- **System-Bausteine (APP):**
  - Client Anwendungen (Desktop, Web, Mobile)
  - Verzeichnisdienst
  - Netzbasierte Dienste (Web, File Server)
  - Business Anwendungen (SAP, Datenbanken)
  - E-Mail, Groupware, Kommunikation)
  - Allgemeine Software
  - Individualsoftware



## IT Grundschutz (Allgemein)

- **System-Bausteine (SYS: Server):**
  - Windows-Server
  - Linux-Server
  - Virtualisierung
  - Containererisierung
  - IGM Z
  - Speicherlösungen

## IT Grundschutz (Allgemein)

- **System-Bausteine (SYS: Desktop):**
  - Windows-Clients (XP, 7,8,10,11)
  - Unix-, Linux-Clients
  - iOS-Clients
- **System-Bausteine (SYS: Mobile):**
  - Laptops
  - Allgemeine Tablet, Smartphones
  - Mobile Device Management (MDM)
  - iOS (Enterprise)
  - Android
  - Mobile Telefon



## IT Grundschutz (Allgemein)

- **System-Bausteine (Netze):**
  - Netzarchitektur
  - Netzdesign
  - **Funknetze (Net.2 WLAN, Net.3.3 VPN)**
  - Netzkomponenten
    - Router
    - Switch
    - Firewall
    - VPN
  - Telekommunikation
    - TK-Anlagen
    - VoIP
    - Fax

## Ebene Leitung

- **Vorgaben für die Sicherheit**
  - Eigene Sicherheitsgrundsätze (Sicherheitsleitlinien)
  - Vorgaben aus Gesetzen, Kundenverträge, Konzernvorgaben)
  - Bereiche siehe IT_Grundschutz_Kompendium_Edition2022.pdf
- **Personal**
  - IT-Sicherheitsbeauftragten (mit Vertreter)
  - IT-Sicherheitsstab, Abteilung (größere Firma)
  - Pro Abteilung ein Sicherheitskoordinator
- **Resourcen**
  - Mittel für Informationsdienste, Tools, Schulungen, externe Berater, Notfalltraining
  - Zertifizierung
- **Bewertung**
  - 1x jährlich eine Evaluierung



## Ebene IT-Sicherheitsmanagement (konzeptionell)

- **Bestimmen der Risiken für die Geschäftsprozesse im Detail**
- **Bewerten der Sicherheitsmaßnahmen**
  - Alle Maßnahmen haben präventiven Charakter.
  - Reichen Sie aus, die Risiken zu minimieren?
  - Wo nicht: striktere Maßnahmen treffen.
  - Bestimmen der Restrisiken
  - Notfallplanung
    - Notfallkonzepte
    - Notfallhandbücher
    - Wiederanlaufpläne
- **Ergebnis: Sicherheitskonzept**

## Ebene IT-Sicherheitsmanagement (2. Teil)

- **Überprüfung und Überwachung der Sicherheit**
  - Tests:
    - Testen der Firewall
    - Ersatzanlagen (Server, Netzwerk, Laptop)
  - Inspektionen
    - Personelle und organisatorische Maßnahmen
  - Auswertung von Aufzeichnungen
    - Zugriffs- und Zutrittsprotokolle
  - Audits
    - Prüfung des aktuellen Zustands (intern oder extern)
  - Messungen (Ermitteln von Kennzahlen, ISO 27004)
    - Der Grad der Erfüllung von Anforderungen
    - Kosten vs. Nutzen
    - Anzahl der Mitarbeiter, die ein mobiles Gerät haben (%)
    - Anzahl der Mitarbeiter, die an einer Schulung teilnahmen (Sensibilisierung^, sollte >90% sein)
    - Mitarbeiter, die „Probleme“ verursachten (%)
    - Datenbackup (wie oft vs. empfohlenen Intervall)



## IT-Grundschutz-Kompendium

- **APP.1.4: Mobile Anwendungen (Apps)**

**1.2 Zielsetzung**

- Ziel dieses Bausteins ist es, Informationen zu schützen, die auf mobilen Endgeräten mit Apps verarbeitet werden.
- Auch die Einbindung von Apps in eine bestehende IT-Infrastruktur wird dabei betrachtet.
- Der Baustein definiert zudem Anforderungen, um Apps richtig auszuwählen und sicher betreiben zu können.
- Dabei werden die Apps unabhängig von ihrer Quelle (App Store oder eigene Installation) betrachtet.

## APP.1.4: Mobile Anwendungen (Apps)

**1. 3 Abgrenzung und Modellierung**

- Der Baustein betrachtet Apps unter mobilen Betriebssystemen wie iOS /Android.
- Anforderungen:
  - Bausteine SYS.3.2.3 iOS (for Enterprise) sowie SYS.3.2.4 Android.
- Mobile Device Management verwaltet: Baustein SYS.3.2.2 MDM
- Backend-Systeme oder Server:
  - APP.3.1 Webanwendungen, APP.3.5 Webservices oder APP.4.3 DBS
- Allgemeinen Aspekte von Anwendungen befassen
  - OPS.1.1.6 SoftwareTests und -Freigaben
  - APP.6 Allgemeine Software
- Eigene Apps
  - Baustein CON.8 Software-Entwicklung



## APP.1.4: Mobile Anwendungen (Apps)

**2. 1 Gefährdungslage**

- Ungeeignete Auswahl von Apps.
  - Besonders hoch ist die Gefahr, wenn es sich dabei um Apps handelt, die nicht eigens für die abzubildenden Geschäftsprozesse entwickelt wurden.
  - Es sind nicht alle für den Betrieb einer App erforderlichen Voraussetzungen geprüft wurden
  - Die mobile Netzanbindung ist nicht leistungsfähig genug oder die Hardware nicht kompatibel.
  - Apps können auch dann ungeeignet sein, wenn sie keine ausreichende langfristige Einsatzstabilität und -planung bieten
  - oder vom Hersteller nicht ausreichend gepflegt werden

## APP.1.4: Mobile Anwendungen (Apps)

**2.2 Zu weitreichende Berechtigungen**

- Berechtigungen pro App einschränken
- Die meisten benötigen eine Internetverbindung
- Den Standort benötigen nicht alle.
- Das Adressbuch sollten nur wenige bekommen.
- Apps können Informationen an Dritte weiterleiten
  - Standort, Fotos, Kontaktdaten, Kalenderdaten
- Apps können kosten verursachen (SMS versenden (GPS), App-Käufe)
- Apps können Daten verändern oder löschen
- **Freischalten beim Benutzen (nicht immer möglich)**



## APP.1.4: Mobile Anwendungen (Apps)

**2.3 Ungewollte Funktionen in Apps**

- Die App-Store Prüfungen sind nicht sicher
  - Sicherheitslücken, enthalten Schadfunktionen
- Problem bei Apps aus ungeprüfter Quelle

**2.4 Software-Schwachstellen und Fehler in Apps**

- Apps können Schwachstellen enthalten, über die sie direkt am Gerät oder über Netzverbindungen angegriffen werden können.
- **Außerdem werden viele Apps nach einiger Zeit von ihren Entwicklern nicht mehr weiter gepflegt.**
- Dadurch werden erkannte Sicherheitsmängel nicht mehr durch entsprechende Updates behoben.

## APP.1.4: Mobile Anwendungen (Apps)

**2.5 Unsichere Speicherung lokaler Anwendungsdaten**

- Einige Apps speichern Daten auf dem Endgerät, beispielsweise Benutzerprofile oder Dokumente. Falls diese Daten unzureichend geschützt sind, können möglicherweise andere Apps darauf zugreifen.
- Dies betrifft neben bewusst abgelegten Daten auch temporäre Daten, wie beispielsweise im Cache zwischengespeicherte Informationen.
- Auch sind sie für Unberechtigte leicht lesbar, z. B. wenn ein Mitarbeiter sein Gerät verloren hat. Außerdem werden lokal gespeicherte Informationen oft nicht im Datensicherungskonzept berücksichtigt.
- Fällt das Endgerät aus oder geht verloren, sind die lokal gespeicherten Informationen ebenfalls nicht mehr verfügbar.



## APP.1.4: Mobile Anwendungen (Apps)

**2.6 Ableitung vertraulicher Informationen aus Metadaten**

- Durch Apps sammeln sich viele Metadaten an.
- Mithilfe dieser Metadaten können Dritte auf vertrauliche Informationen schließen, z. B. über Telefon- und Netzverbindungen, Bewegungsdaten oder besuchte Webseiten.
- Daraus lassen sich dann weitere Informationen ableiten, beispielsweise die Organisationsstruktur der Institution, genaue Positionen von Standorten sowie deren personelle Besetzung.

## APP.1.4: Mobile Anwendungen (Apps)

**2.7 Abfluss von vertraulichen Daten**

- Daten werden über verschiedene Wege von und zu einer App übertragen. Dafür stellen mobile Betriebssysteme verschiedene Schnittstellen bereit.
- Der Benutzer hat ebenfalls verschiedene Möglichkeiten, Daten mit einer App
- auszutauschen, etwa lokal über eine Speicherkarte, die Zwischenablage, die Gerätekamera oder andere Anwendungen. Außerdem können Daten über Cloud-Dienste oder Server des App- oder Geräte-Anbieters übertragen
- werden.
- Darüber können Dritte Zugriff auf die vertraulichen Daten erlangen.
- Schließlich kann auch das Betriebssystem selbst Daten für den schnelleren Zugriff zwischenspeichern (Caching). Dabei können Daten versehentlich abfließen oder Angreifer auf vertrauliche Informationen zugreifen.



## APP.1.4: Mobile Anwendungen (Apps)

**2.8 Unsichere Kommunikation mit Backend-Systemen**

- Viele Apps kommunizieren mit Backend-Systemen, über die Daten mit dem Datennetz der Institution ausgetauscht werden.
- Die Daten werden bei mobilen Geräten zumeist über unsichere Netze wie ein Mobilfunknetz oder WLANHotspots übertragen.
- Werden für die Kommunikation mit Backend-Systemen aber unsichere Protokolle verwendet, können Informationen abgehört oder manipuliert werden

## APP.1.4: Mobile Anwendungen (Apps)

**2.9 Kommunikationswege außerhalb der Infrastruktur der Institution**

- Wenn Apps unkontrolliert mit Dritten kommunizieren können, kann dies Kommunikationswege schaffen, die nicht von der Institution erkannt und kontrolliert werden können.
- So kann ein Benutzer beispielsweise die App eines Cloud-Datenspeicherdienstes nutzen, um Informationen vom Endgerät nach außen zu übertragen.
- Auch die enge Verzahnung von Social-Media-Diensten mit vielen Apps erschwert die Kontrolle, ob und wie Informationen das Endgerät verlassen.
- Diese Art von Kommunikationswegen sind nur schwer nachzuvollziehen. Dies kann noch weitere Probleme verursachen, etwa wenn der Anwender oder die Institution verpflichtet sind, Informationen oder Vorgänge zu archivieren



## APP.1.4: Mobile Anwendungen (3 Anforderungen)

**APP.1.4.A5 Minimierung und Kontrolle von App-Berechtigungen**

- Sicherheitsrelevante Berechtigungseinstellungen MÜSSEN so fixiert werden, dass sie nicht durch Benutzer oder Apps geändert werden können.
- Wo dies technisch nicht möglich ist, MÜSSEN die Berechtigungseinstellungen regelmäßig geprüft und erneut gesetzt werden.
- Bevor eine App in einer Institution eingeführt wird, MUSS sichergestellt werden, dass sie nur die minimal benötigten App-Berechtigungen für ihre Funktion erhält. Nicht unbedingt notwendige Berechtigungen MÜSSEN hinterfragt und gegebenenfalls unterbunden werden.

## APP.1.4: Mobile Anwendungen (3 Anforderungen)

**APP.1.4.A7 Sichere Speicherung lokaler App-Daten**

- Wenn Apps auf interne Dokumente der Institution zugreifen können, MUSS sichergestellt sein, dass die lokale Datenhaltung der App angemessen abgesichert ist.
- Insbesondere MÜSSEN Zugriffsschlüssel verschlüsselt abgelegt werden.
- Außerdem DÜRFEN vertrauliche Daten NICHT vom Betriebssystem an anderen Ablageorten zwischengespeichert werden

**APP.1.4.A8 Verhinderung von Datenabfluss**

- Um zu verhindern, dass Apps ungewollt vertrauliche Daten versenden oder aus den gesendeten Daten Profile über die Benutzer erstellt werden, MUSS die App-Kommunikation geeignet eingeschränkt werden.
- Dazu SOLLTE die Kommunikation im Rahmen des Test- und Freigabeverfahrens analysiert werden. Weiterhin SOLLTE überprüft werden, ob eine App ungewollte Protokollierungs- oder Hilfsdateien schreibt, die möglicherweise vertrauliche Informationen enthalten.



## APP.1.4: Mobile Anwendungen (3 Anforderungen)

**APP.1.4.A14 Unterstützung zusätzlicher Authentisierungsmerkmale bei Apps**

- Falls möglich, SOLLTE für die Authentisierung der Benutzer in Apps ein zweiter Faktor benutzt werden. Hierbei SOLLTE darauf geachtet werden, dass eventuell benötigte Sensoren oder Schnittstellen in allen verwendeten Geräten vorhanden sind.
- Zusätzlich SOLLTE bei biometrischen Verfahren berücksichtigt werden, wie resistent die Authentisierung gegen mögliche Fälschungsversuche ist.

**APP.1.4.A15 Durchführung von Penetrationstests für Apps**

- Bevor eine App für den Einsatz freigegeben wird, SOLLTE ein Penetrationstest durchgeführt werden.
- Dabei SOLLTEN alle Kommunikationsschnittstellen zu Backend-Systemen sowie die lokale Speicherung von Daten auf mögliche Sicherheitslücken untersucht werden. Die Penetrationstests SOLLTEN regelmäßig und zusätzlich bei größeren Änderungen an der App wiederholt werden.

# APP.1.4: Mobile Anwendungen (5 Gefährdungen)

- G 0.9 Ausfall oder Störung von Kommunikationsnetzen
- G 0.14 Ausspähen von Informationen (Spionage)
- G 0.15 Abhören
- G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten
- G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten
- G 0.18 Fehlplanung oder fehlende Anpassung
- G 0.19 Offenlegung schützenswerter Informationen
- G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle
- G 0.21 Manipulation von Hard- oder Software
- G 0.23 Unbefugtes Eindringen in IT-Systeme
- G 0.25 Ausfall von Geräten oder Systemen
- G 0.26 Fehlfunktion von Geräten oder Systemen
- G 0.28 Software-Schwachstellen oder -Fehler
- G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen
- G 0.32 Missbrauch von Berechtigungen
- G 0.36 Identitätsdiebstahl
- G 0.38 Missbrauch personenbezogener Daten
- G 0.39 Schadprogramme
- G 0.42 Social Engineering



| Elementare Gefährdungen / Anforderungen | CIA-Werte | G 0.9 | G 0.14 | G 0.15 | G 0.16 | G 0.17 | G 0.18 | G 0.19 | G 0.20 | G 0.21 | G 0.23 | G 0.25 | G 0.26 | G 0.28 | G 0.31 | G 0.32 | G 0.36 | G 0.38 | G 0.39 | G 0.42 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| APP.1.4.A1 | | X | X | X | X | X | X | X | | | | X | X | | | | | X | | |
| APP.1.4.A2 | | | | | | | | | | | | | | | | | | | | |
| APP.1.4.A3 | | | X | | | | X | X | X | X | X | | | | | X | | | X | |
| APP.1.4.A4 | | | | | | | | | | | | | | | | | | | | |
| APP.1.4.A5 | | | X | X | | | | X | | X | | | | | | X | | X | X | X |
| APP.1.4.A6 | | | | | | | | | | | | | | | | | | | | |
| APP.1.4.A7 | | | X | | X | X | | X | | | | | | | | | | | | |
| APP.1.4.A8 | | | X | X | | | | X | | | | | | | | | | X | | |
| APP.1.4.A9 | | | | | | | | | | | | | | | | | | | | |
| APP.1.4.A10 | | | | | | | | | | | | | | | | | | | | |
| APP.1.4.A11 | | | | | | | | | | | | | | | | | | | | |
| APP.1.4.A12 | | | X | | | | X | X | | | | | | | | | | X | | |
| APP.1.4.A13 | | | | | | | | | | | | | | | | | | | | |
| APP.1.4.A14 | CI | | X | | X | X | X | X | | | X | | | | | X | X | | | |
| APP.1.4.A15 | CIA | | | | | | | | | X | X | X | X | X | | | | | | |
| APP.1.4.A16 | CIA | | | | | | X | | | | | | | | X | | | | | |