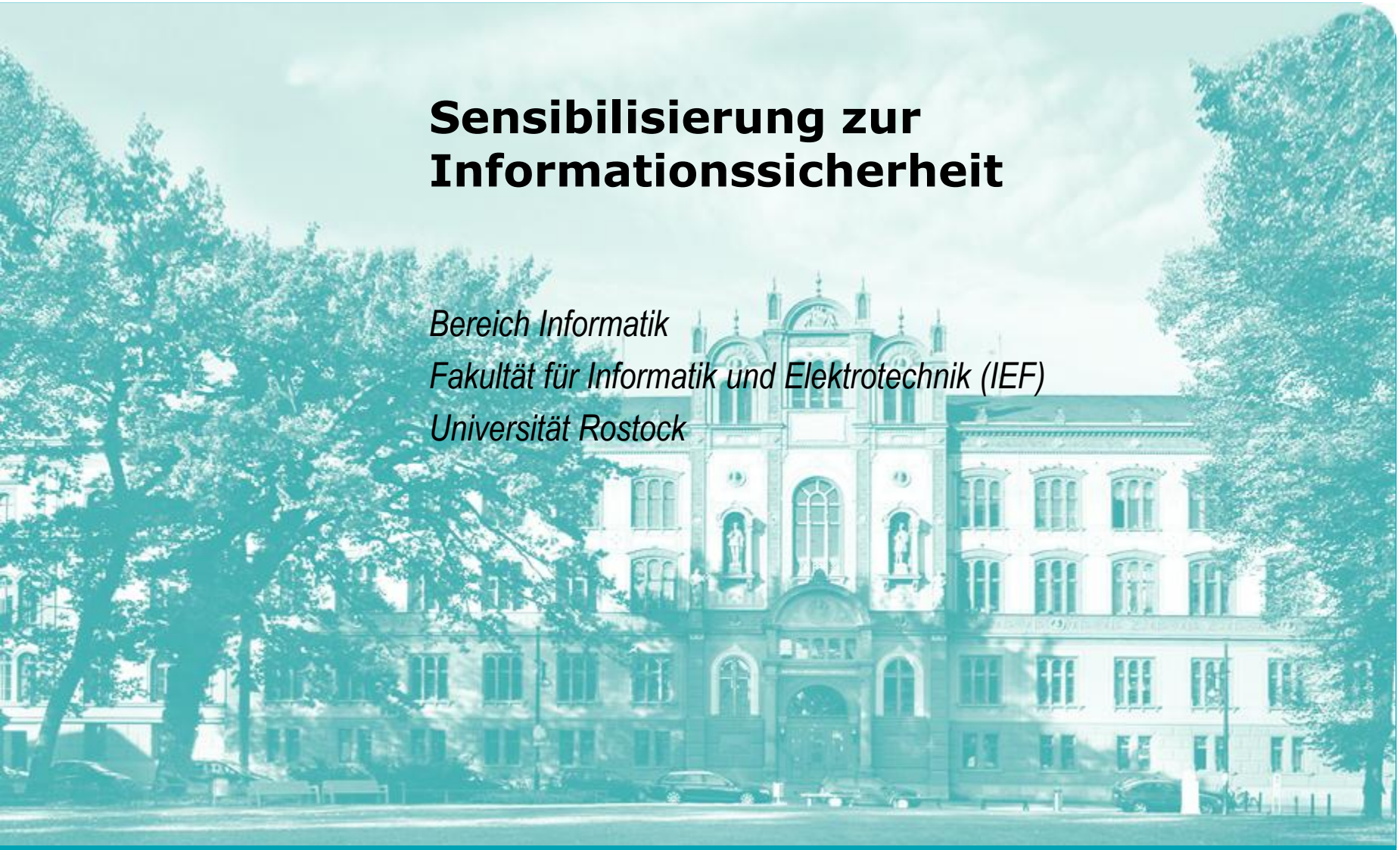
Universität Rostock

Traditio et Innovatio

Sensibilisierung zur Informationssicherheit

Bereich Informatik
Fakultät für Informatik und Elektrotechnik (IEF)
Universität Rostock



Inhalte

Stand: 27.03.2025

1. Allgemeines
2. Sicherer Arbeitsplatz und sichere IT-Infrastruktur
3. Sicherheit für mobile Geräte
4. Passwörter
5. Vertrauliche Daten
6. Umgang mit Sicherheitsvorfällen

Quellen:

- Uni Rostock, IT-Sicherheitskonzept für das ITMZ: https://www.itmz.uni-rostock.de/it-sicherheit/dokumente-und-links/it-sicherheitskonzept-fuer-das-itmz/
- TU München, Infos und Tipps zur IT-Sicherheit für Mitarbeiter/innen: https://www.it.tum.de/it/it-sicherheit/fuer-mitarbeiterinnen/
- security.org – How Secure Is My Password? https://www.security.org/how-secure-is-my-password/

Allgemeines

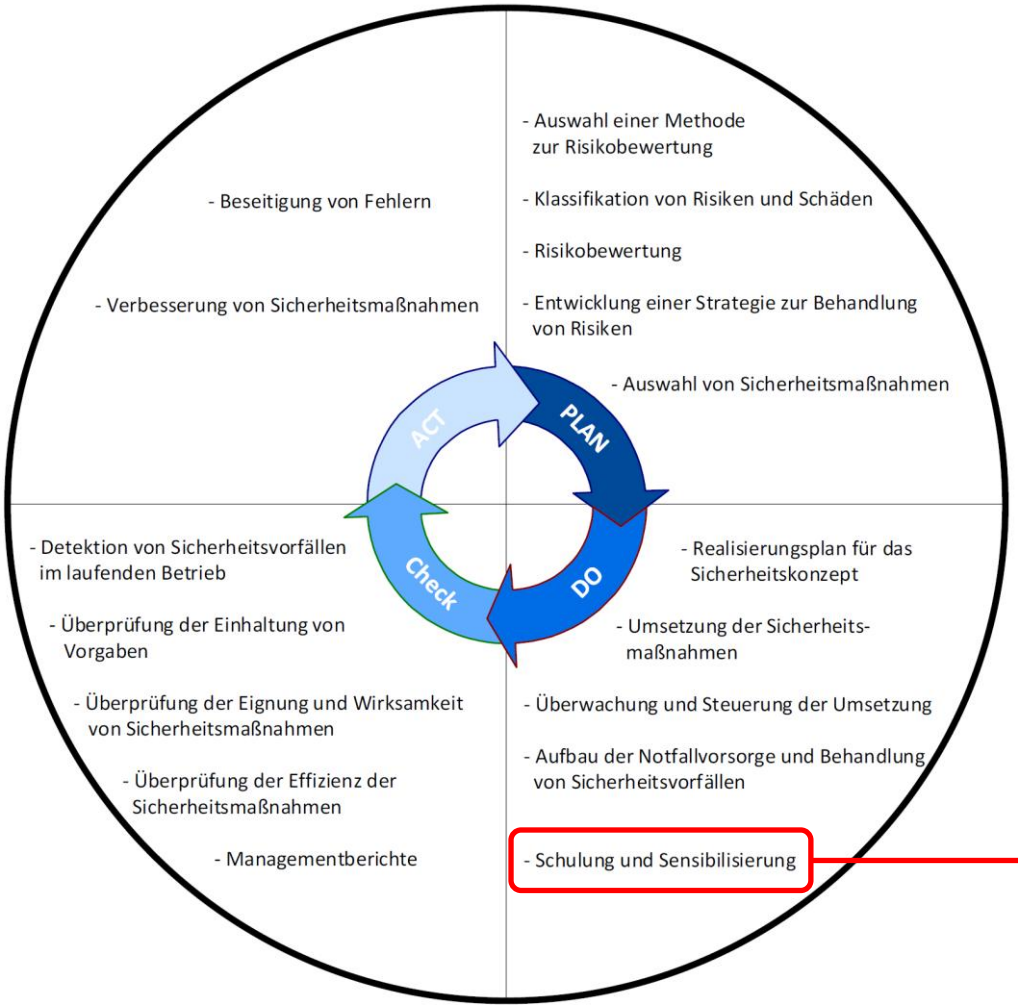
Informationssicherheit ist unverzichtbar.

- Systematisches Management der Informationssicherheit zum Schutz von Daten, Informationen und IT-Systemen notwendig in Bezug auf:
  - **Vertraulichkeit** *(en.: Confidentiality)*: Sensible oder vertrauliche Informationen werden vor unbefugter Preisgabe geschützt.
  - **Unversehrtheit/Integrität** *(en.: Integrity)*: Alle Daten bleiben während und vor allem nach ihrer Verarbeitung vollständig und unverändert.
  - **Verfügbarkeit** *(en.: Availability)*: Dem Benutzer stehen alle Informationen und Funktionalitäten des Systems zum richtigen Zeitpunkt zur Verfügung.

- Nützliche kostenlose Online-Schulung: https://training.linuxfoundation.org/training/cybersecurity-essentials-lfc108/

IT-Sicherheitskonzept der Uni Rostock

Lebenszyklus des ITMZ-Sicherheitskonzeptes



Orientiert sich an der Methodik des BSI-Grundschutzes.

Schulung und Sensibilisierung

Sicherer Arbeitsplatz und sichere IT-Infrastruktur

Klare Verantwortlichkeiten für Betriebssysteme und Anwendungen

- Systemingenieur ist verpflichtend zuständig und verantwortlich für Betriebssysteme und Anwendungen der IT-Infrastruktur
- Teilbereiche können durch qualifizierte Mitarbeitende übernommen werden

Sicherer Arbeitsplatz und sichere IT-Infrastruktur

Schutz vor Zugriff durch andere Personen & Schadsoftware

- **Computer sperren** (Bildschirmschoner mit Passwortsperre oder Win+L)
  - auch bei nur kurzem Verlassen des Arbeitsplatzes!
- Software sparsam installieren und nicht verwendete Software deinstallieren
  - gilt auch für Browsererweiterungen
- Kein Administratorkonto für die tägliche Arbeit nutzen, nur bei Bedarf

- Software aktuell halten: **Updates installieren**
  - für das Betriebssystem (Windows, macOS, Linux, etc.)
  - für alle verwendeten Programme (z.B. Browser)
- Virenschutz und Firewall des Betriebssystems aktivieren und aktiviert lassen

Sicherer Arbeitsplatz und sichere IT-Infrastruktur

Verdächtige E-Mails und USB-Sticks

- Vorsicht bei **verdächtigen E-Mails**
  - Absender überprüfen, auf Externe-E-Mail-Warnung achten
  - Plausibilität der Mail prüfen, insbesondere bei „dringenden“ Aufforderungen
  - Anhänge nur von vertrauenswürdigen Absendern öffnen, Dateityp überprüfen

- Vorsicht bei **fremden USB-Sticks**
  - Schadsoftware und -hardware kann als USB-Stick getarnt sein
    - Bsp.: Gerät tut so, als wäre es eine Maus/Tastatur und imitiert den Nutzer
  - Keine USB-Sticks unbekannter Herkunft anschließen oder verwenden

Sicherer Arbeitsplatz und sichere IT-Infrastruktur

Webseiten und Werbung

- Sicheres Surfen
  - Bekannte und vertrauenswürdige Webseiten bevorzugen
  - **Authentizität** der Webseiten überprüfen
    (insbesondere Schreibweise der Adresse: unirostock.de statt uni-rostock.de?)
  - Auf **Verschlüsselung** achten (https://... bzw. Schloss-Symbol)
  - Downloads ausschließlich von vertrauenswürdigen Quellen

- Vorsicht vor **Werbeanzeigen** (Werbebanner, Pop-Ups etc. auf Webseiten)
  - Vermeintliche Werbung kann Schadsoftware oder Phishing-Versuche enthalten
  - Werbeblocker wie *uBlock Origin* installieren

Sicherer Arbeitsplatz und sichere IT-Infrastruktur

Backup und Wiederherstellung

- Keine privaten Daten auf Arbeitsgeräten speichern
- Schutz Ihrer Daten vor Verlust und Zerstörung
  - Daten nicht lokal, sondern auf Netzlaufwerk der Universität speichern
  - Bei lokalen Daten: **Backups** erstellen und Wiederherstellung **testen**!
- Rechner kompromittiert (oder Verdacht darauf)?
  - **Achtung:** Keine Daten von kompromittierten Systemen mehr sichern!
  - Daten können infiziert sein und neues / bereinigtes Gerät erneut kompromittieren

Sicherheit für mobile Geräte

Allgemeine Sicherheitshinweise

- Herausgabe der eigenen Mobilfunknummer nur wenn nötig
- Unbekannte Rufnummern vor dem Rückruf verifizieren
  (insbesondere auf teure Sonderrufnummern wie 0900… oder Auslandsvorwahl achten)

- Apps ausschließlich aus vertrauenswürdigen Quellen installieren
  (Apple App Store, Google Play Store)
- **Updates installieren:** für das Betriebssystem und alle Apps
- Bei Verlust von SIM-Karten oder Geräten mit eSIM-Profilen: Sofort Karte und/oder Gerät **sperren** lassen!

Sicherheit für mobile Geräte

Aufbewahrung und Weitergabe

- Geräte (Handys / Tablets / Laptops / etc.) nicht unbeaufsichtigt lassen
  - Unbeaufsichtigte Geräte sind schnell gestohlen
  - oder: Schadsoftware kann schnell und unbemerkt installiert werden!
- Geräte nicht aus der Hand geben
- Verlust / Diebstahl von Geräten **melden**

- *Shoulder Surfing:* Mitlesen von Inhalten auf Bildschirmen „über die Schulter“
  - Sichtschutzfolien (Privacy Filter) schränken den Blickwinkel des Displays ein
  - Wahl eines Sitzplatzes mit Rücken zur Wand
- Vertrauliche Gespräche nur an ruhigen, privaten Orten führen, ggf. zurückrufen

Sicherheit für mobile Geräte

Geräte vor fremdem Zugriff schützen

- Bildschirmsperre aktivieren und mit **PIN** oder **Passwort** sichern
  - SIM-PIN ≠ Geräte-PIN: SIM-PIN schützt nur Mobilfunk, nicht das ganze Gerät
  - zusätzlich **Biometrie** möglich: Fingerabdruck / 3D-Gesichtserkennung

- Speicher von Geräten vollständig verschlüsseln
  - Standard bei iOS und ab Android 6.0 mit PIN oder Passwort
  - Windows: BitLocker aktivieren, Linux: dm-crypt + LUKS einrichten
  - macOS: Standard mit T2- oder Apple-Chips, sonst FileVault aktivieren

Sicherheit für mobile Geräte

Sichere Nutzung von öffentlichen WLANs und Geräten

- Offene (passwortlose) WLANs sind meistens **unverschlüsselt**
  - Datenverkehr kann ohne weitere Schutzmaßnahmen (z.B. HTTPS) mitgelesen werden, Angreifer können das Netzwerk imitieren und manipulieren
  - WLANs mit öffentlich bekannten Passwörtern sollten ebenfalls wie unverschlüsselt behandelt werden
  - **Aktivieren des Uni-VPNs** mit Profil *Internet-Access* sofort nach Herstellung der WLAN-Verbindung (auch bei verschlüsselten WLANs)
  - WLAN nach der Nutzung aus der Liste bekannter Netzwerke **löschen**, um automatische Verbindung zu verhindern
- Bei der Nutzung öffentlicher Geräte (auch *CleverTouch*): Keine sensiblen Daten eingeben oder speichern (z.B. Passwörter), sonstige gespeicherte Daten löschen

Passwörter

Ein langes Passwort ist stärker als ein kurzes, komplexes Passwort!

- **Passwortlänge:** mindestens 10 Zeichen, besser 16 Zeichen
  - 8 Kleinbuchstaben: Ermittelt in 5 Sekunden
  - 10 Kleinbuchstaben: Ermittelt in 1 Tag
  - 16 Kleinbuchstaben: Ermittelt in 4.000 Jahren
- **Passwortkomplexität:** Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen
  - 10 Klein- & Großbuchstaben: Ermittelt in 1 Monat
  - + Zahlen: Ermittelt in 7 Monaten
  - + Sonderzeichen: Ermittelt in 5 Jahren
- **Kombination:** Lange und komplexe Passwörter sind praktisch nicht zu erraten
  - Komplexes Passwort mit 16 Zeichen: Ermittelt in 10^{12} (1 Billion) Jahren

Passwörter

Lange Passwörter sind nicht sicher, wenn sie leicht erraten werden können!

- Die besten Passwörter sind zufällige Zeichenketten, sodass alle Möglichkeiten durchprobiert werden müssen, um sie zu erraten (**Brute-Force-Angriff**)

- **Wörterbuchangriffe** nutzen folgende Schwächen aus, um Passwörter deutlich schneller als auf der letzten Folie gezeigt zu ermitteln:
  - *Persönliche Daten* wie Namen, Geburtstage, Autokennzeichen als Passwort
  - *Ganze Wörter*, die in normalen Wörterbüchern vorkommen (auch rückwärts oder mit durch Zahlen ersetzte Zeichen wie „p4ssw0rt“)
  - *Tastaturmuster* wie „qwertz“ oder „asdf1234“ usw.
  - Listen der *häufigsten* oder *zuvor kompromittierter* Passwörter, z.B.: 123456, passwort, hallo, hallo123, super123, daniel, michael, …

Passwörter

Sichere Aufbewahrung

- **Passwortmanager** wie *Bitwarden* oder *KeePass* verschlüsseln und schützen Passwörter sicher mit einem einzigen auswendig gelernten **Hauptpasswort**
- **Niemals:** Passwörter unverschlüsselt speichern oder Merkzettel an Bildschirm, Schreibtisch, unter der Tastatur, etc. anbringen!

- Passwörter **ändern**, wenn System oder Administratoren dazu auffordern
- **Aber:** Niemals Passwörter *weitergeben* (Admins werden nie Ihr Passwort benötigen!)

Passwörter

Finden und Merken guter Passwörter

- **Unterschiedliche Passwörter** für unterschiedliche Dienste verwenden
  - insbesondere Trennung zwischen privat und dienstlich
- Passwortmanager können sichere Passwörter für jeden Dienst **automatisch erzeugen**
- Zur **manuellen Erzeugung** sicherer Passwörter: Einen langen, leicht zu merkenden Satz wählen und Anfangsbuchstaben, Zahlen und Sonderzeichen zusammenfassen
  - „Ich kaufe T-Shirts seit Anfang 2013 nur noch online“ → „IkT-SsA2013nno“
  - Keine populären Zitate oder Liedtexte verwenden! (Wörterbuchangriffe)

Vertrauliche Daten

Alle Daten, die nicht für die Öffentlichkeit bestimmt sind.

- **(sensible) Personenbezogene Daten:** Stammdaten von Mitarbeitern, Studierenden, Bewerbern; Zugangskennungen, Passwörter, Nutzungsprotokolle
  - besonderer Schutz durch Datenschutzgesetze

- **Geistiges Eigentum:** Nicht veröffentlichtes Forschungsmaterial, urheberrechtlich geschützte Inhalte in Unterrichtsmaterialien
  - Schutzmaß durch Forschende bzw. Urheber/-innen festgelegt

- **Geschäftskritische Daten:** strategische Dokumente, Daten zum Rechnungswesen, Daten zu Stiftungen, etc.
  - nur wenige ausgewählte Personen mit Zugriff, sonst stark zu schützen

Vertrauliche Daten

Umgang mit vertraulichen Daten

- **Erfassung:** *Datensparsamkeit* – so wenig Daten wie möglich, nur so viele Daten wie nötig erfassen. Daten, die nicht gesammelt wurden, müssen nicht geschützt werden.

- **E-Mails:** Nur an bekannte Empfänger und Adressen @uni-rostock.de senden
  - **Als Empfänger:** E-Mails nicht an private Adressen weiterleiten lassen
  - **Verschlüsselung:** Bei personenbezogenen oder geschäftskritischen Daten müssen E-Mails verschlüsselt werden!

- **Cloud:** Ausschließlich Netzwerk- und Cloud-Speicher und der Uni Rostock verwenden, keine Ablage auf öffentlichen oder externen Cloud-Speichern

Vertrauliche Daten

Signieren und Verschlüsseln von E-Mails

- **Signieren** von E-Mails schützt vor Identitätsdiebstahl
  - Absenderfeld in unsignierten E-Mails ist leicht zu manipulieren
  - Korrekte Signatur bestätigt Absender und Integrität der Nachricht
- **Verschlüsseln** von E-Mails schützt vertrauliche Daten vor unbefugtem Zugriff
  - E-Mails sind standardmäßig unverschlüsselt
  - Verschlüsselung per Zertifikat beschränkt Zugriff auf gewünschte Empfänger

Vertrauliche Daten

Nutzerzertifikat beantragen

➢ https://zertifikate.uni-rostock.de

- **Einfache** Zertifikate eignen sich zum Verschlüsseln und Signieren von E-Mails
- **Erweiterte** Zertifikate eignen sich zusätzlich zum Signieren von Dokumenten
  - Identitätsprüfung durch ITMZ-Mitarbeiter notwendig (siehe Website)

- Anleitung vom ITMZ: https://www.itmz.uni-rostock.de/it-sicherheit/zertifikate-und-verschluesselung/zertifikate-fuer-nutzer/zertifikat-beantragen/

Vertrauliche Daten

Nutzerzertifikat in E-Mail-Programm einrichten

- Anleitungen vom ITMZ für Outlook, Apple Mail und Mozilla Thunderbird
- Outlook Web Client (https://email.uni-rostock.de) ist nicht geeignet

➢ Zum Signieren: https://www.itmz.uni-rostock.de/onlinedienste/e-mail-und-kollaboration/e-mail/e-mail-sicherheit/e-mails-signieren/

➢ Zum Verschlüsseln: https://www.itmz.uni-rostock.de/onlinedienste/e-mail-und-kollaboration/e-mail/e-mail-sicherheit/e-mails-verschluesseln/

Vertrauliche Daten

Zu meidende Mailprogramme

- Aufgrund von Speicherung der Anmelde- und Postfachdaten in der Microsoft-Cloud sind aus Datenschutzgründen folgende Mailprogramme nicht zu empfehlen:
  1. Neues Microsoft Outlook (2024)
  2. Outlook für Android
  3. Outlook für iOS

- Alternativen sind auf der Seite des ITMZ zu finden

Vertrauliche Daten

Datenschutz bei der Erhebung von Studierendendaten

- Zentrale Systeme der Uni Rostock werden datenschutzrechtlich zentral verwaltet, selbst beschaffte oder externe Systeme hingegen nicht

- Verantwortliche Person(en) für den Betrieb eigener Software und die Datenverarbeitung klären und von Datenschutzbeauftragten freigeben lassen
- Bei externen Systemen den Anbieter per **Auftragsdatenverarbeitungsvertrag** (AVV) an datenschutzrechtlich relevante Aspekte binden
  - Ist das nicht möglich, dürfen betroffene Dienste nicht verwendet werden!
  - Daten besser auf zentralen oder eigenen internen Servern speichern
- Bei eigenen öffentlichen **Webanwendungen:** Impressum und Datenschutzerklärung!

Vertrauliche Daten

Online-Dienste

- **Terminplanung:** DFN-Terminplaner – https://terminplaner6.dfn.de/
- **Chat:** Rocket.Chat der Uni Rostock – https://chat.uni-rostock.de/
- **Meetings:** Zoom X auf Servern der dt. Telekom – https://uni-rostock-de.zoom.us/
- **LaTeX-Dokumente:** Overleaf der Uni Rostock – https://overleaf.uni-rostock.de/
- **Cloud:** Unibox der Uni Rostock – https://unibox.uni-rostock.de/

Vertrauliche Daten

Drucker

- Viele ausgedruckte Dokumente sind vertraulich, auch in anderen Dokumenten finden sich oft personenbezogene Daten: Drucker und Ausdrucke müssen geschützt werden!

- **Drucker können speichern:** Druckaufträge werden oft auf internen Speichern im Drucker länger zwischengelagert und sind unverschlüsselt!
- **Netzwerkdrucker sind angreifbar:** Zugriff auf Drucker von außerhalb per Firewall verhindern, oftmals keine Authentifizierung zur Nutzung von Druckern nötig
- **Druckaufträge sofort abholen:** Ausdrucke, die länger in Druckern liegen, können prinzipiell von jedem mitgenommen werden. Wenn möglich: Physischen Zugang zu Druckern beschränken.

Umgang mit Sicherheitsvorfällen

Definition „Sicherheitsvorfall“

- Umfasst jede **Beeinträchtigung** der drei Schutzziele für vertrauliche Daten
  - *Vertraulichkeit:* Daten wurden veröffentlicht oder Unbefugten zugänglich
    - E-Mail an falsche Person(en) gesendet / weitergeleitet
    - Passwörter gestohlen, Zugriff auf Daten mit fremdem Konto
    - Zutrittsberechtigungen zu Räumen und Gebäuden missbraucht
  - *Integrität:* Daten wurden manipuliert, gelöscht oder (falsche) Daten hinzugefügt
    - Prüfungsdaten mit gestohlenen Zugangsdaten verändert, Protokolle gelöscht
  - *Verfügbarkeit:* Zugang zu Daten unmöglich
    - Systemausfall durch Angriff oder Fehler (nicht: geplante Wartungsarbeiten)
    - Daten, Passwörter oder Zutrittsberechtigungen verloren

Umgang mit Sicherheitsvorfällen

Definition „Schwerwiegender Sicherheitsvorfall“

- Beispiele für schwerwiegende Vorfälle:
  - Manueller Angriff auf Universitätssysteme von intern oder extern
  - Zugangsdaten für Nutzerkonten sind eventuell Unbefugten bekannt
  - Angreifer bewegen sich über infizierte Geräte durch das Universitätsnetzwerk
  - Zutrittsberechtigungen wurden gestohlen und/oder missbraucht

- Beispiele für nicht schwerwiegende Vorfälle:
  - Erfolglose Social-Engineering-Angriffe, infizierte E-Mails
  - Erfolglose Login-Versuche von außerhalb des Universitätsnetzwerks

Umgang mit Sicherheitsvorfällen

Meldekette

- Alle Sicherheitsvorfälle an zuständige/-n Systemingenieur/-in melden!

- Bei Phishing-E-Mails oder infizierten E-Mails:
  Weitergabe an Postmaster der Universität (postmaster@uni-rostock.de)
- Bei *potenziell* schwerwiegenden Fällen: zusätzlich Institutsleitung und IT-Sicherheitsbeauftragten per E-Mail informieren (it-sicherheit@uni-rostock.de)
- Bei *gesichert* schwerwiegenden Fällen: ITMZ telefonisch informieren (5301)
  - ITMZ behandelt nur Account- / Netzsperren und Log-Sichtung

Umgang mit Sicherheitsvorfällen

Sofortmaßnahmen

- **Verbreitung verhindern:** Kompromittierte Geräte vom Netzwerk trennen
  - Netzwerkkabel entfernen
  - WLAN deaktivieren, falls möglich
  - Gerät bis zur Freigabe durch IT-Sicherheit nicht mehr verwenden
- **Zugang blockieren:** Passwörter ändern
  - Insbesondere, wenn gleiche Passwörter für mehrere Dienste genutzt werden
  - Kein kompromittiertes Gerät zur Passwortänderung verwenden!
  - Konto kann ggf. durch ITMZ gesperrt werden, um Missbrauch zu verhindern