OTH Amberg-Weiden

Cybersicherheit

Einführung

Prof. Dr. Daniel Loebenberger

Amberg, 02. Oktober 2024

Hinweis

OTH Amberg-Weiden

- Bitte beachten Sie das Urheberrecht!
- Alle Materialien dieser Vorlesung sind – auch wenn sie nicht ausdrücklich gekennzeichnet sind – urheberrechtlich geschützt.
- Sie dienen ausschließlich Ihrem persönlichen Gebrauch im Rahmen dieser Vorlesung.
- Die Materialien dürfen insbesondere nicht weiter verbreitet werden.
- Eigene Aufzeichnungen (Video, Foto, Ton) der Vorlesung sind nicht gestattet.

Gliederung

OTH Amberg-Weiden

1. Einführung
2. Kryptographie
3. Netzwerksicherheit
4. Systemsicherheit
5. Anwendungssicherheit
6. Kritische Infrastrukturen und staatlicher Geheimschutz
7. Sicherheitsmodelle und -evaluierung
8. Sicherheit im Unternehmen
9. Hacking und Pentesting (extern)
10. Ausblick

Überblick

OTH Amberg-Weiden

01 Organisatorisches

02 Struktur der Vorlesung

03 IT-Sicherheit vs. Cybersicherheit

04 Aufstellen eines Sicherheitsproblems

Überblick

OTH Amberg-Weiden

Termine

OTH Amberg-Weiden

Vorlesung

- Mittwoch, 08:00h – 09:30h und 09:45h – 11:15h
- Hörsaal EMI108, Fakultät EMI, Campus Amberg
- Ggf. teilweise remote via BigBlueButton (via Moodle)

Übungen

Übungen jeweils nach relevanten Themenblöcken.

Webseite/Kommunikation

OTH Amberg-Weiden

Moodle Plattform

`https://moodle.oth-aw.de`, Einschreibeschlüssel `CYBER$3C`

Am besten heute noch einschreiben (falls nicht geschehen)!

Weitere Kommunikationsmedien

- Hier in Präsenz im Hörsaal :)
- Per E-Mail an `d.loebenberger@oth-aw.de`
- Im BigBlueButton Raum

Kursmaterialien (I)

OTH Amberg-Weiden

Folien

Zu jedem Kapitel gibt es Foliensätze

- Auf der Moodle-Webseite zu finden
- Handout-Version mit ausreichend Platz zum Schreiben
- Bitte melden Sie gefundene Unklarheiten, inhaltliche Fehler, Typos etc.

Sprechstunde

Jeweils nach der Vorlesung oder nach Vereinbarung per E-Mail.

Kursmaterialien (II)

OTH Amberg-Weiden

Übungen

Aktive Teilnahme erforderlich:

- Studium von Zusatzliteratur
- Folien mit Übungsaufgaben zu den einzelnen Themen
- Dazu kommen praktische Übungen
- Dafür sinnvoll: Zugang zu einem Linux-basierten System, z.B. Fedora (`https://getfedora.org/de/`)
- Installation direkt oder z.B. via VirtualBox (`https://www.virtualbox.org`)

Stellen Sie Fragen!

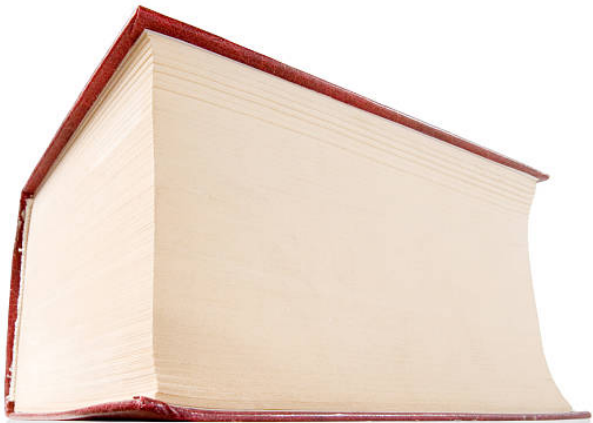
Benotung

OTH Amberg-Weiden

Prüfung

- Schriftliche Prüfung
- Voraussichtlich am 22.01.2025 anstelle der letzten Vorlesung
- 90 Minuten Bearbeitungszeit
- Eine Woche vorher (15.01.2025): Fragestunde

Literatur



Quelle: alexfiodorov, www.istockphoto.com

Literatur

Bücher:

- C. Eckert. IT-Sicherheit: Konzepte - Verfahren - Protokolle. De Gruyter Studium. De Gruyter, 2018. ISBN: 978-3-1105-8468-4
- James F. Kurose und Keith W. Ross. Computernetzwerke: Der Top-Down-Ansatz. Pearson Deutschland GmbH, 2008. ISBN: 978-3-8689-4237-8
- Jon Erickson. Hacking: the art of exploitation. No starch press, 2008. ISBN: 978-1-5932-7144-2
- Daniel Regalado u. a. Gray Hat Hacking: The Ethical Hacker's Handbook. McGraw-Hill Education New York, 2015. ISBN: 978-1-5848-8543-6
- Fabiano Dalpiaz, Elda Paja und Paolo Giorgini. Security requirements engineering: designing secure socio-technical systems. MIT Press, 2016. ISBN: 978-0-2620-3421-0

Immer nützlich:

- Wikipedia. URL: `https://de.wikipedia.org`

Überblick

OTH Amberg-Weiden

Themen der Vorlesung
(vorläufig)

OTH Amberg-Weiden

1. Einführung
2. Kryptographie
3. Netzwerksicherheit
4. Systemsicherheit
5. Anwendungssicherheit
6. Kritische Infrastrukturen und staatlicher Geheimschutz
7. Sicherheitsmodelle und -evaluierung
8. Sicherheit im Unternehmen
9. Hacking und Pentesting (extern)
10. Ausblick

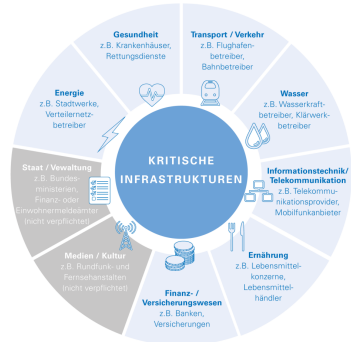
Überblick

OTH Amberg-Weiden

Was ist eigentlich Cybersicherheit?

Motivation

- Zur Absicherung technischer Systeme müssen Schutzziele der Informationssicherheit erfüllt werden
- Unterscheide funktionale und kryptographische Schutzziele
- Funktionale Schutzziele: korrekter (und sicherer) Betrieb
- Kryptographische Schutzziele: Einschränkung des Zugriffs
- Technologische Basis sind kryptographische Verfahren
  - Verschlüsselungsverfahren
  - Schutz vor Manipulation
  - Schutz des Absenders
- Besonderer Anwendungsfall: kritische Infrastrukturen



Quelle: TÜV Rheinland

Schutzziele

OTH Amberg-Weiden

Verfügbarkeit	System erfüllt Anforderungen an Funktionalität
Vertraulichkeit	Daten dürfen nur von autorisierten Benutzern gelesen werden
Integrität	Daten dürfen nicht unbemerkt verändert werden
Authentizität	Die Herkunft der Daten darf nicht unbemerkt verändert werden
Verbindlichkeit	Durchgeführte Berechnungen können nicht abgestritten werden
Zurechenbarkeit	Es muss einen eindeutige Zuordnung von Daten möglich sein
Anonymität	Die Herkunft der Daten darf nicht offengelegt werden
...	Je nach Anwendungsfall weitere Ziele denkbar

Ziele schließen teilweise einander aus!

Schutzziele: Beispielanwendung

OTH Amberg-Weiden

Notwendiger Schutz:

- Verfügbarkeit
- Vertraulichkeit
- Integrität
- Authentizität
- Verbindlichkeit
- Zurechenbarkeit
- Anonymität

IoT-Sensor

Schutzziele: Beispielanwendung

OTH Amberg-Weiden

Notwendiger Schutz:

- ✔ Verfügbarkeit
- ✘ Vertraulichkeit
- ✘ Integrität
- ✘ Authentizität
- ✘ Verbindlichkeit
- ✘ Zurechenbarkeit
- ✘ Anonymität

Temperatur-Messung

Schutzziele: Beispielanwendung

OTH Amberg-Weiden

Notwendiger Schutz:

- ✔ Verfügbarkeit
- ✔ Vertraulichkeit
- ✔ Integrität
- ✔ Authentizität
- ✘ Verbindlichkeit
- ✔ Zurechenbarkeit
- ✘ Anonymität

Temperatur-Messung im Kernkraftwerk

Schutzziele: Beispielanwendung

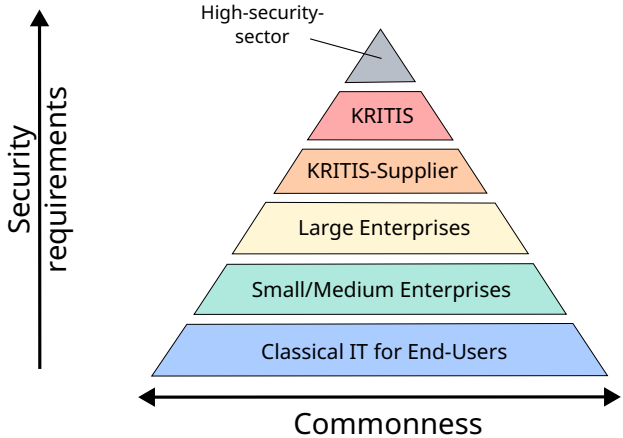
OTH Amberg-Weiden

Notwendiger Schutz:

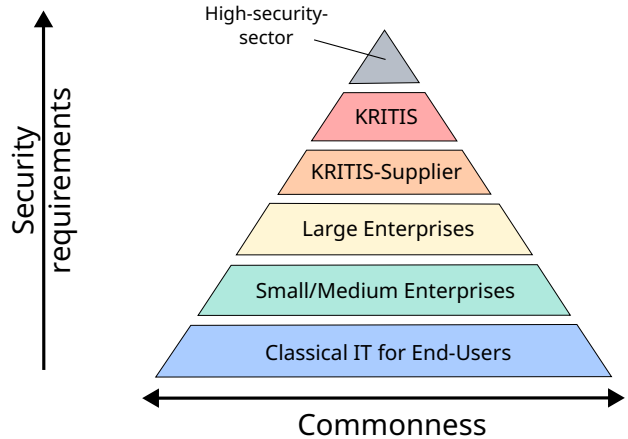
- ✔ Verfügbarkeit
- ✔ Vertraulichkeit
- ✔ Integrität
- ✔ Authentizität
- ✔ Verbindlichkeit
- ✘ Zurechenbarkeit
- ✔ Anonymität

Sensor
(paranoider Ansatz)

Sicherheitsanforderungen

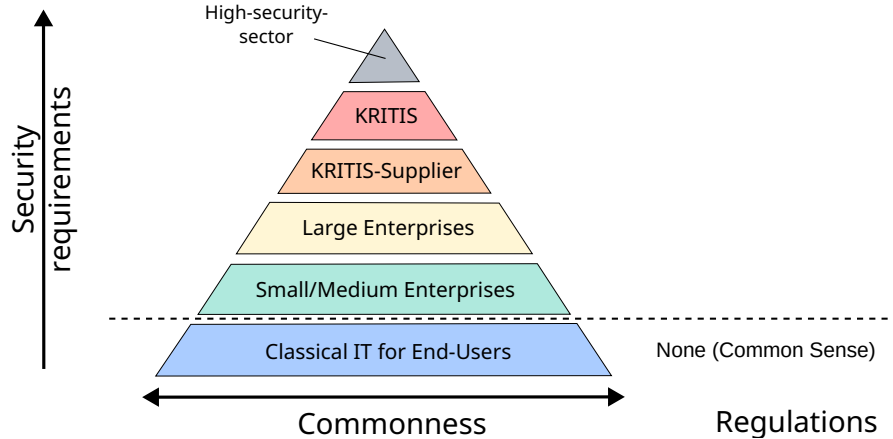


Sicherheitsanforderungen

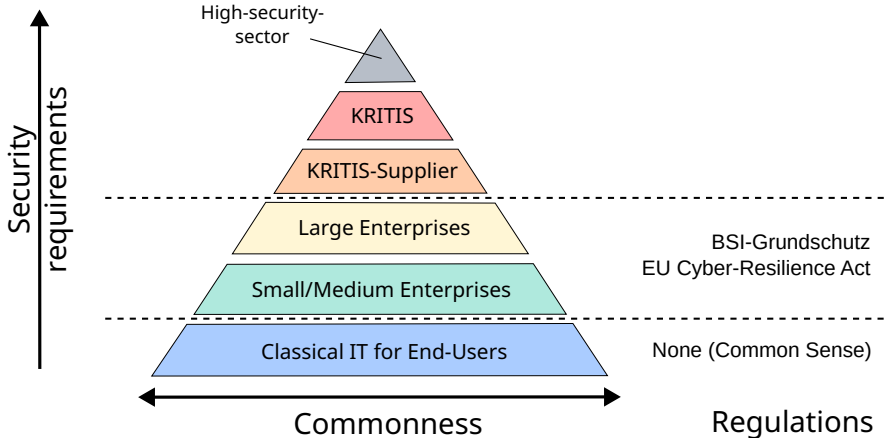


Regulations

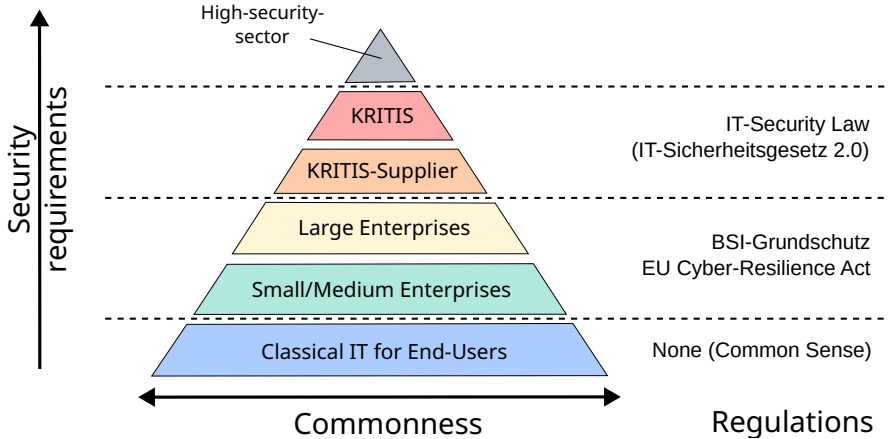
Sicherheitsanforderungen



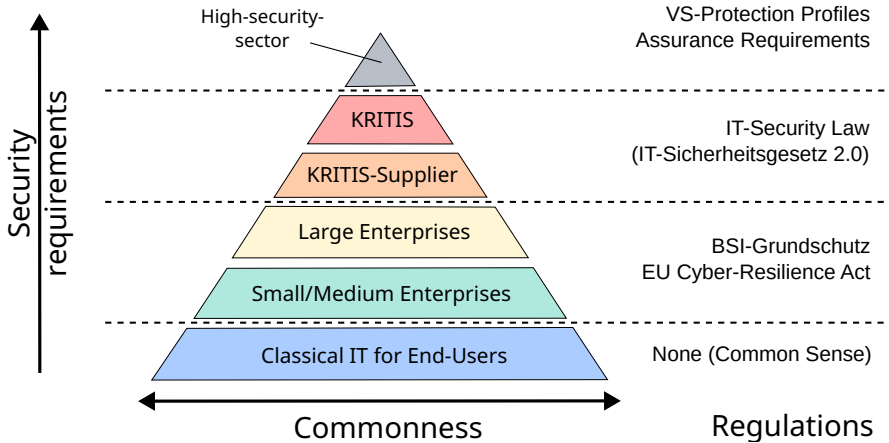
Sicherheitsanforderungen



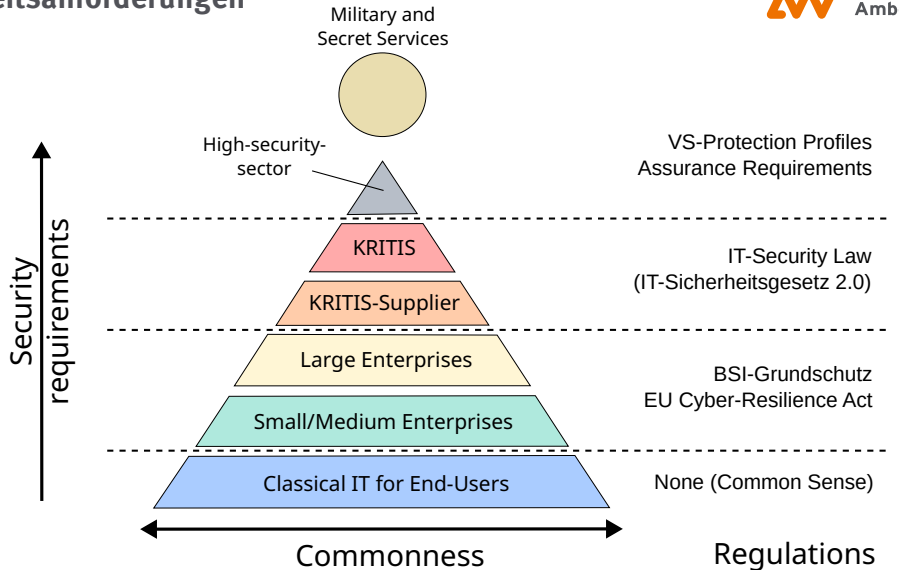
Sicherheitsanforderungen



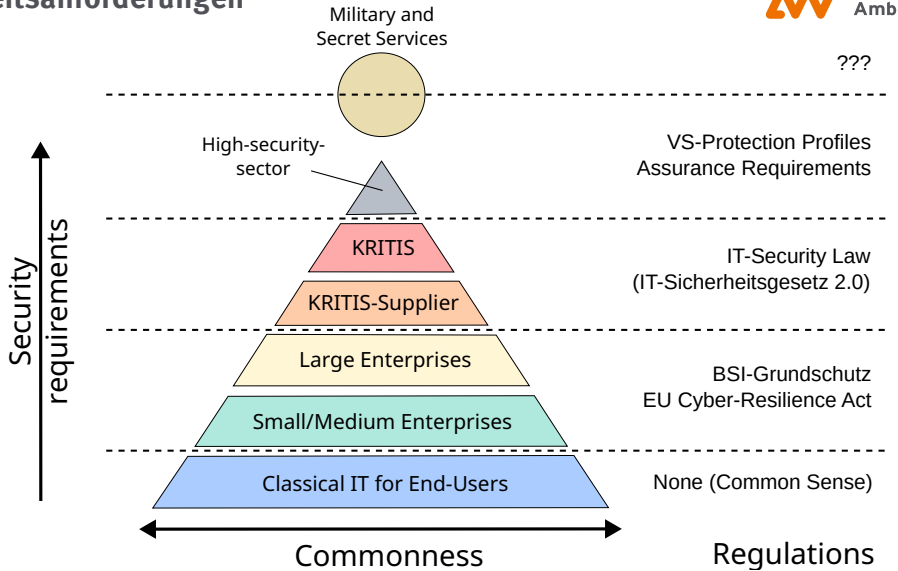
Sicherheitsanforderungen



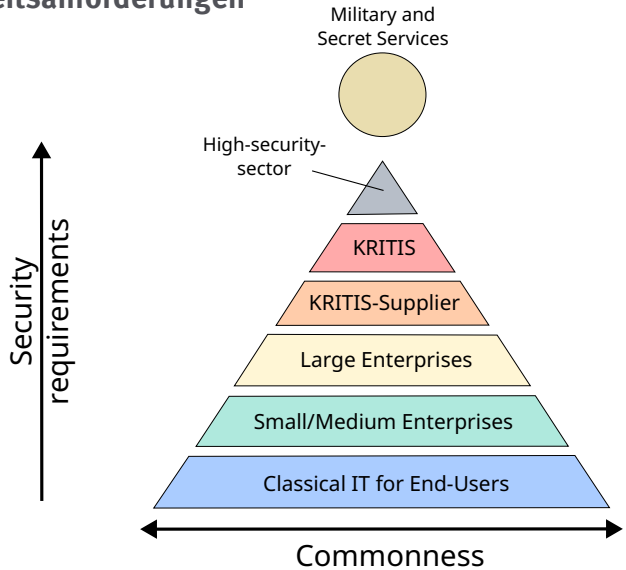
Sicherheitsanforderungen



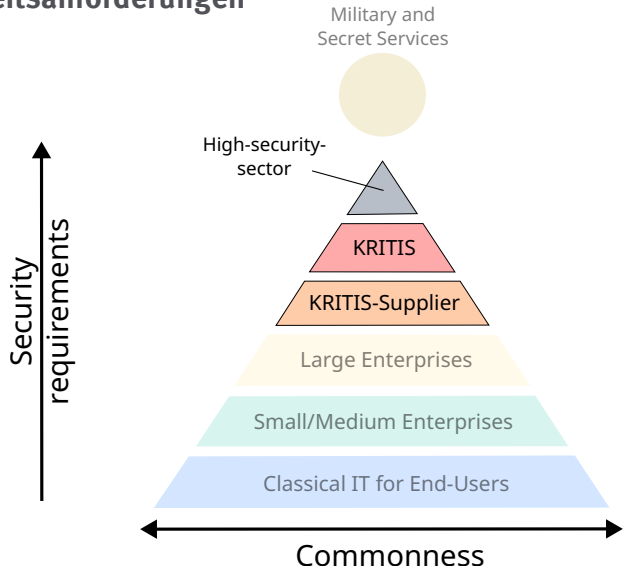
Sicherheitsanforderungen



Sicherheitsanforderungen



Sicherheitsanforderungen

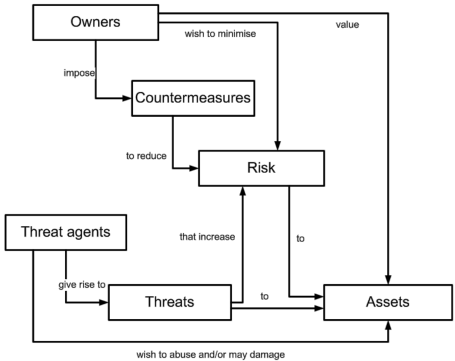


Wie zeigt man, dass ein IT-System sicher ist?

Überblick

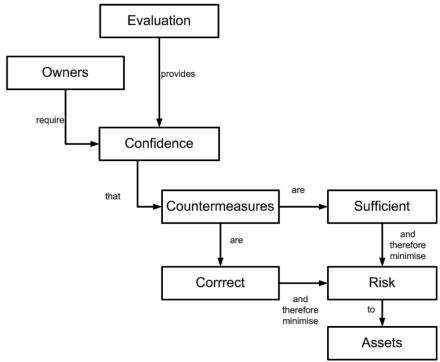
OTH Amberg-Weiden

Sicherheitsmodell
Abhängigkeiten



Quelle: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general mode. Version 3.1, Revision 5. Apr. 2017. URL: https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf

Sicherheitsmodell
Evaluation



Quelle: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general mode. Version 3.1, Revision 5. Apr. 2017. URL: https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf

Sicherheitsproblem
Definitionen

OTH Amberg-Weiden

Rollen	Kommunikationsteilnehmer
Werte	Zu schützende Informationen
Bedrohungen	Potenzielle Angriffe auf die Werte
Sicherheitsziele	Gegenmaßnahmen, welche die Bedrohungen abwehren sollen
Sicherheitsfunktionen	Technische Realisierung der Sicherheitsziele
Annahmen	Sicherheitsziele, die nicht technisch realisiert werden können

Übungsaufgaben

OTH Amberg-Weiden

1.1.1. Nehmen Sie für die folgenden Aufgaben an, dass das IT-System funktionssicher ist:

(a) Beschreiben Sie ein IT-System, welches keines der Schutzziele erfüllt.
(b) Nennen Sie ein IT-System, welches Vertraulichkeit, aber sonst kein anderes Ziel erfüllt.
(c) Nennen Sie ein IT-System, welches Integrität, Authentizität, Verbindlichkeit und Anonymität gewährleistet.
(d) Nennen Sie ein IT-System, welches alle der obigen Schutzziele mit Ausnahme der Anonymität gewährleistet.

1.1.2. Betrachten Sie die Formulierung eines Sicherheitsproblems für die sichere Übertragung von E-Mails.

(a) Nennen Sie typische Rollen bei der Übertragung von E-Mails.
(b) Welche schützenswerten Werte fallen Ihnen ein?
(c) Nennen Sie beispielhaft zwei Bedrohungen der von Ihnen genannten Werte.
(d) Welche Sicherheitsziele können Sie definieren, um den Bedrohungen zu begegnen?
(e) Durch welche Maßnahmen können Sie diese technisch realisieren?

1.1.1

a) LED-streifen, Waschmachine, 3D-Drucker, Notstrom, Roboterarm

b) verschlüsselte Datei/Email/Festplatte

c) Bitcoin-Netzwerk, Blockchain

d) Banküberweisungen, TLS/VPN-Kommunikation

1.1.2

a) Sender, Empfänger, Internet-Provider, Email-Provider?, Angreifer

b) Email Inhalt, Email-Adressen, IP-Adressen

c) Phishing, Spam, Viren etc., Email, Email-Passwort

d) Authentifizierung, Integrität, Vertraulichkeit

e) Mails verschlüsseln, Firewall, Spamfilter, 2FA

Gibt es Fragen?