Wodurch entstehen
Gefahren?
- Nicht ausreichende Zugriffskontrolle
- Fehlkonfigurationen
- Schwachstellen in der Software
- Mangelnde Überwachung
- Ausfall oder Verlust der Kontrolle von Daten

Phishing
- Gefälschte Emails, Nachrichten oder Websites
- Nutzer gibt Anmeldeinformationen preis oder ladet bösartige Dateien herunter

Man in the Middle (MITM)
- Angreifer mischen sich zwischen zwei Personen oder Geräten ein
- Meistens durch
- ARP Spoofing
- Wifi-Hotspot Angriff

Insider Bedrohungen
- Gefahr innerhalb einer Organisation
- Person die absichtlich Daten verkauft
- Person die versehentlich eine schädliche Email öffnet

Internet of Things Bedrohungen
- Sicherheitsrisiken in vernetzten Geräten
- Smart-Home oder Industriesteuerungssysteme die nicht ausreichend geschützt sind
- Nützlich für DDoS oder stehlen persönlicher Daten

DDoS - Angriff
- Große Anzahl an Geräten sendet gleichzeitig Anfragen an Website oder Server
- Führt zu Überlastung
- Website oder Server wird für den normalen Nutzer unzugänglich

Firmware Angriffe
- Die Software wird angegriffen
- Router oder Smartphones
- Ermöglicht meist langfristigen Zugang zu den Geräten

Cryptojacking
- Die elektrische Energie/Rechenleistung wird heimlich genutzt
- Farmen von Kryptowährungen

Schwachstellen in Cloud Services

- Sicherheitslücken in Clouddiensten
- Angreifer haben Zugriff auf sensible Daten

Was kann man machen um das Risiko zu minimieren?

- Regelmäßige Aktualisierung der Software und Patches
- Verschlüsselung von Daten
- Überwachung der Zugriffe und Reaktion auf Sicherheitsvorfälle