KURZPORTRÄT IOT-SECURITY

Nationaler Akademietag 2019
3./4. Mai 2019 in Hamburg

Gliederung

Das Beste zum Schluß

- Rahmenbedingungen
- Inhalt

Einführung

- Version 1.0 | Released Februar 2019
- Instructor-led oder self-paced
- Aufwand: > 70 Stunden mit allen Labs – daher im Rahmen der Module z.B. zum CCNA, aber mehr Übungen als Lesestoff

Kapitelüberblick

- Chapter 1: The IoT Under Attack
- Chapter 2: IoT Systems and Architectures
- Chapter 3: IoT Device Layer Attack Surface
- Chapter 4: IoT Communication Layer Attack Surface
- Chapter 5: IoT Application Layer Attack Surface
- Chapter 6: Vulnerability and Risk Assessment in an IoT System

Inhalt

- Aus der inhaltlichen Gliederung wird klar, dass sich der Kurs schwerpunktmäßig mit der Angriffsfläche der drei Dimensionen:
  - *Device*
  - *Kommunikation*
  - *Applikation*

  auseinandersetzt.
- Ziel ist die Sensibilisierung für das Thema, das Aufzeigen von Angriffsflächen und eine Begegnung der Angriffe auf Modellbasis

Notwendige Tools

- PL-App Launcher (Prototyping Lab Application)
- Image for IoT Security
- Oracle Virtual Box
- Kali VM Image
- Raspberry PI
- Switch

Besonderheiten

- Eine Vielzahl externer Links verweisen auf Web-Sites mit Bezug zu vielen Aspekten der Thematik:
  - *Shodan*
  - *CVSS Calculator* = *Common Vulnerability Scoring System*
  - *Blockchain-Demo*

Leistungsnachweis

- Quiz für jedes Kapitel
- Final Exam

Rahmenbedingungen

- IoT-Netze können sehr viele Komponenten unterschiedlichen Typs enthalten s. nachfolgendes Beispiel.
- IoT-Elemente besitzen einige Restriktionen:
  - *Kleiner Speicher*
  - *Geringe Rechenleistung*
  - *Geringer Stromverbrauch, um die Lebensdauer zu erhöhen*
- Aus den Restriktionen ergeben sich unmittelbar Folgen für die Sicherheitsmöglichkeiten
- Erste Maßnahme: Netzsegmentierung!!

Beispiel: Cisco openBerlin

- Die Räumlichkeiten mit einer Fläche von rund 1.000 m^2 sind mit über 10.000 Sensoren und Hightech-Kommunikation ausgestattet, um möglichst detailliert Informationen zu Licht- und Klimaverhältnissen über Gesichtserkennung bis zu Smartwatches der Mitarbeiter im Gebäude erfassen zu können.
- Die Gebäudeautomation basiert auf einem System von WAGO und ist so ausgelegt, dass sich ohne Eingreifen von außen sowohl die Beleuchtung als auch das Raumklima automatisch auf die optimalen Komfortbedingungen für die Mitarbeiter, Kunden und Partnern einstellen lässt, d.h. Lichtstärke und -farbe verändern sich je nach Jahres- beziehungsweise Tageszeit so, dass die Menschen individuell auf die Nutzung eines Raumes oder Arbeitsplatzes abgestimmt die besten Bedingungen vorfinden.

Gliederung

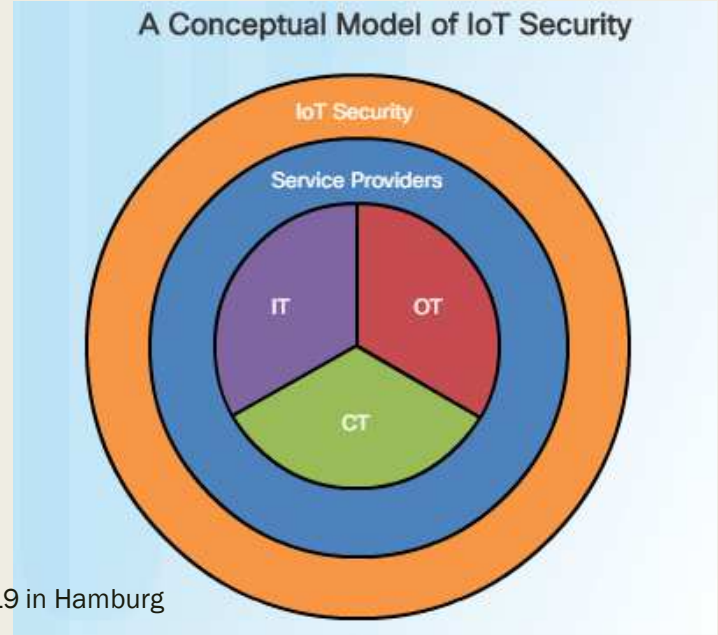
- Rahmenbedingungen
- Inhalt

Chapter 1: Anliegen

- Beschreibung von IoT-Sicherheitsherausforderungen und möglicher Angriffe und deren Folgen im Bereich von Smart Homes und dem Gesundheitswesen:
  - *Anatomie eines Angriffs*
  - *Mirai-Botnet*
- Verschmelzung von IT, OT und CT

Chapter 1: allgemeine Einordnung

- IoT und Security stellen zwei zur Zeit stark diskutierte Begriffe dar – IoT als neue Technologie und Möglichkeit, die Industrie 4.0 zu unterstützen; Security als immer weiter in den Vordergrund rückende Rahmenkomponente.
- Die IT wächst mit der OT (operational technology) und der CT (consumer technology) zusammen, was die Angriffsfläche wesentlich vergrößert, insbesondere auch deshalb, weil die OT vorher weitgehend abgeschottet war.



Chapter 2: Anliegen

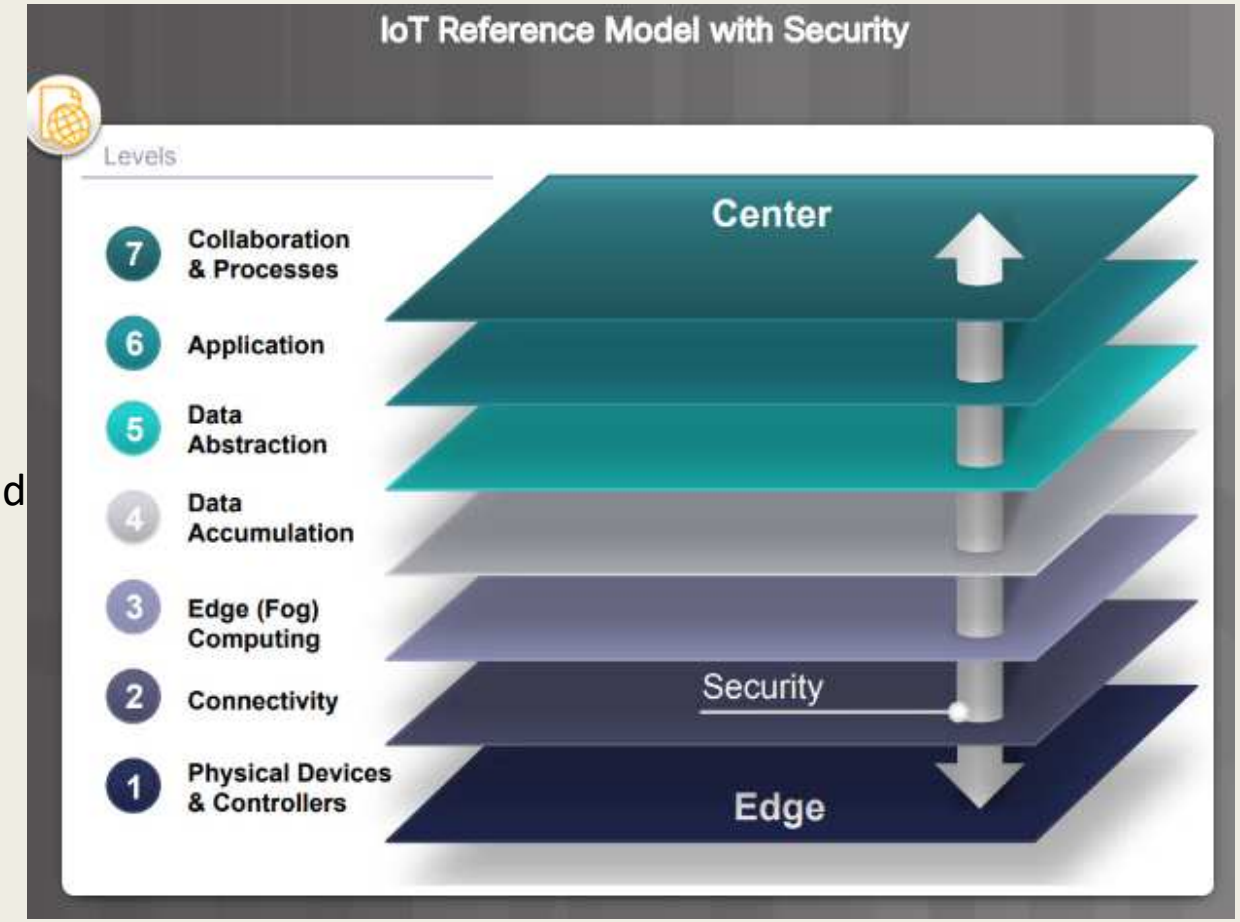
Schaffung allgemeiner Standards und Modelle:

- Bedeutung von IoT-Standards und Architekturen
- Beleuchtung eines IoT-Sicherheitsmodells
- Schaffung eines IoT-Threat-Modells

Chapter 2: IoT-Standard-Referenzmodell

Ein Schichtenmodell:

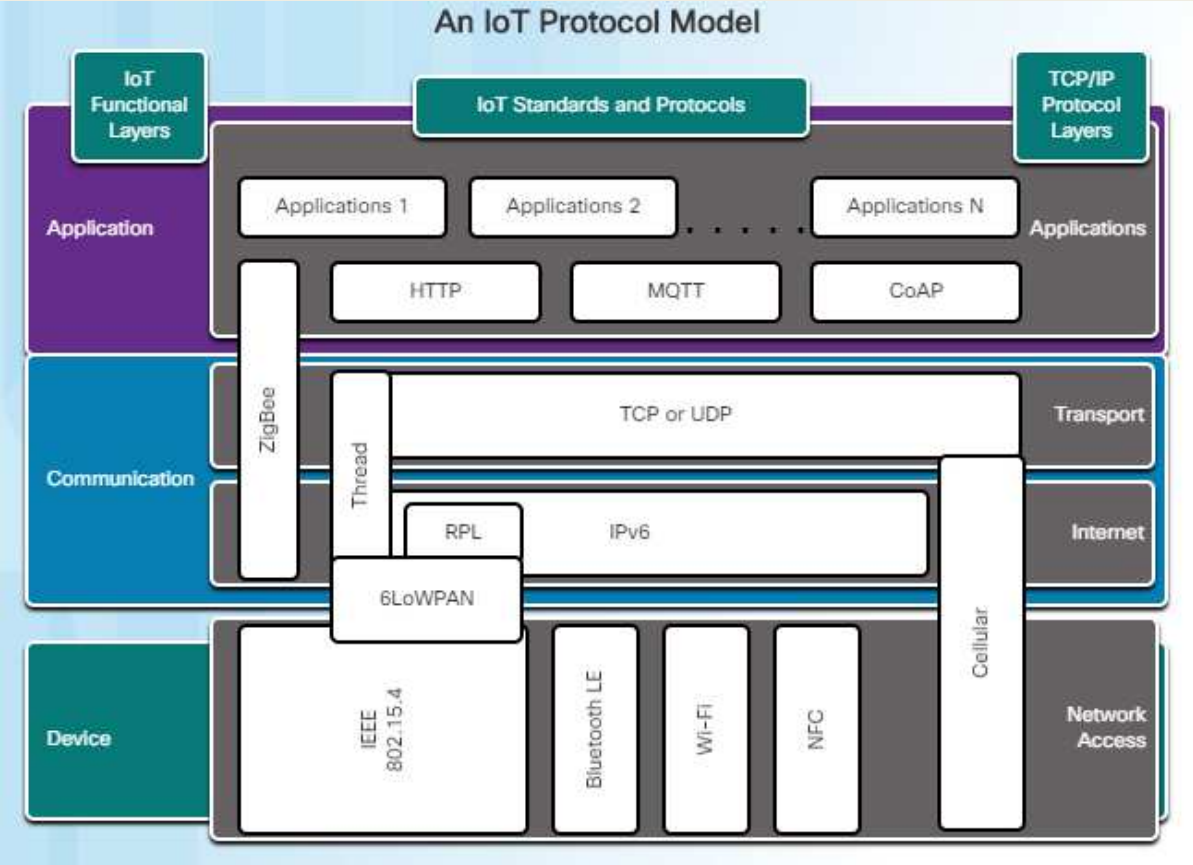
- Bietet Sicherheit für Hard- und Software für jedes Device
- Gewährleistet sichere Prozesse
- Sichert die “Bewegung” von Daten und die Kommunikation



Chapter 2: IoT Security Model

Der Kurs kombiniert die funktionalen Schichten des IoT mit dem TCP/IP-Modell:

- Application: ZigBee, HTTP, MQTT, CoAP
- Communication: TCP/UDP, IPv6
- Device: IEEE 802.15.4, WiFi, 4G und 5G



Chapter 2: NICE Cybersecurity Workforce Framework

- Ausdruck eines Threat-Modells:

Chapter 3: Anliegen

- Überblick über IoT-Devices, Firmware, Betriebssysteme etc.
- Bedrohungsmodellierung durch ein Threat-Modells
- Maßnahmen zur Abwehr von Bedrohungen gegen IoT-Devices

Chapter 3: IoT-Devices

- Constrained Devices
  - *Smart sensors*
  - *Embedded Devices*
- CPU-Typen
  - *RISC*
  - *CISC*
- Memory
  - *SD-Karten*
  - *EPROM*
  - *SRAM/DRAM*
- Ports
  - *Serielle Kommunikation*
  - *EPROM und Mikrocontroller*
- Betriebssysteme
  - *Busybox (Linux-basiert)*
  - *Android Embedded*
  - *Windows 10 IoT*

Chapter 3: Angreifbarkeit

- Physikalische Sicherheit
- Angriffe über Firmware (Default-Login, Pufferüberlauf, nicht aktueller Firmwarestand)

Chapter 3: Gegenmaßnahmen

- Access-Control-Modelle
- OAuth 2.0 Authorization Framework
- Passwortsicherheit
- Verschlüsselung

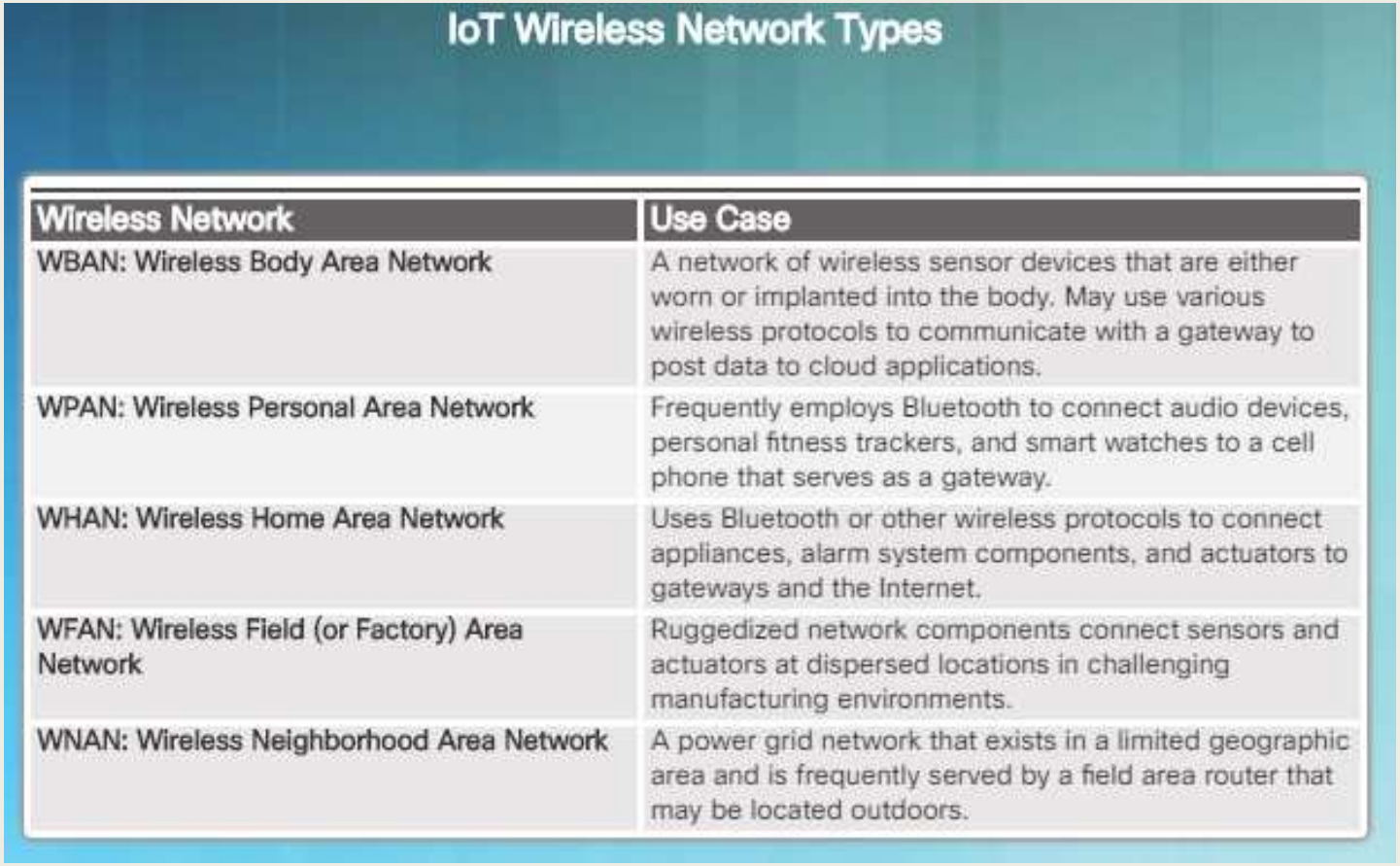
Chapter 4: Anliegen

- Erkennung der Verwundbarkeit der IoT-Kommunikationsschicht und der Wireless-Protokolle
- Beschreibung der Verwundbarkeit von TCP/IP und deren Wirkung auf IoT
- Gegenmaßnahmen

Chapter 4: Angriffsfläche nach dem Open Web Application Security Project (OWASP)

OWASP Communication Layer Vulnerabilities	
Attack Surface	**Vulnerability**
Device Network Services	Information disclosure Injection Denial of Service Unencrypted Services Poorly implemented encryption Test/Development Services Vulnerable UDP Services DoS Replay attack Lack of payload verification Lack of message integrity check
Network Traffic	LAN traffic LAN to Internet traffic Short range Non-standard protocols Wireless (Wi-Fi, Z-wave, XBee, Zigbee, Bluetooth, LoRA) Packet manipulation (protocol fuzzing)

Chapter 4: Wireless-Typen in IoT



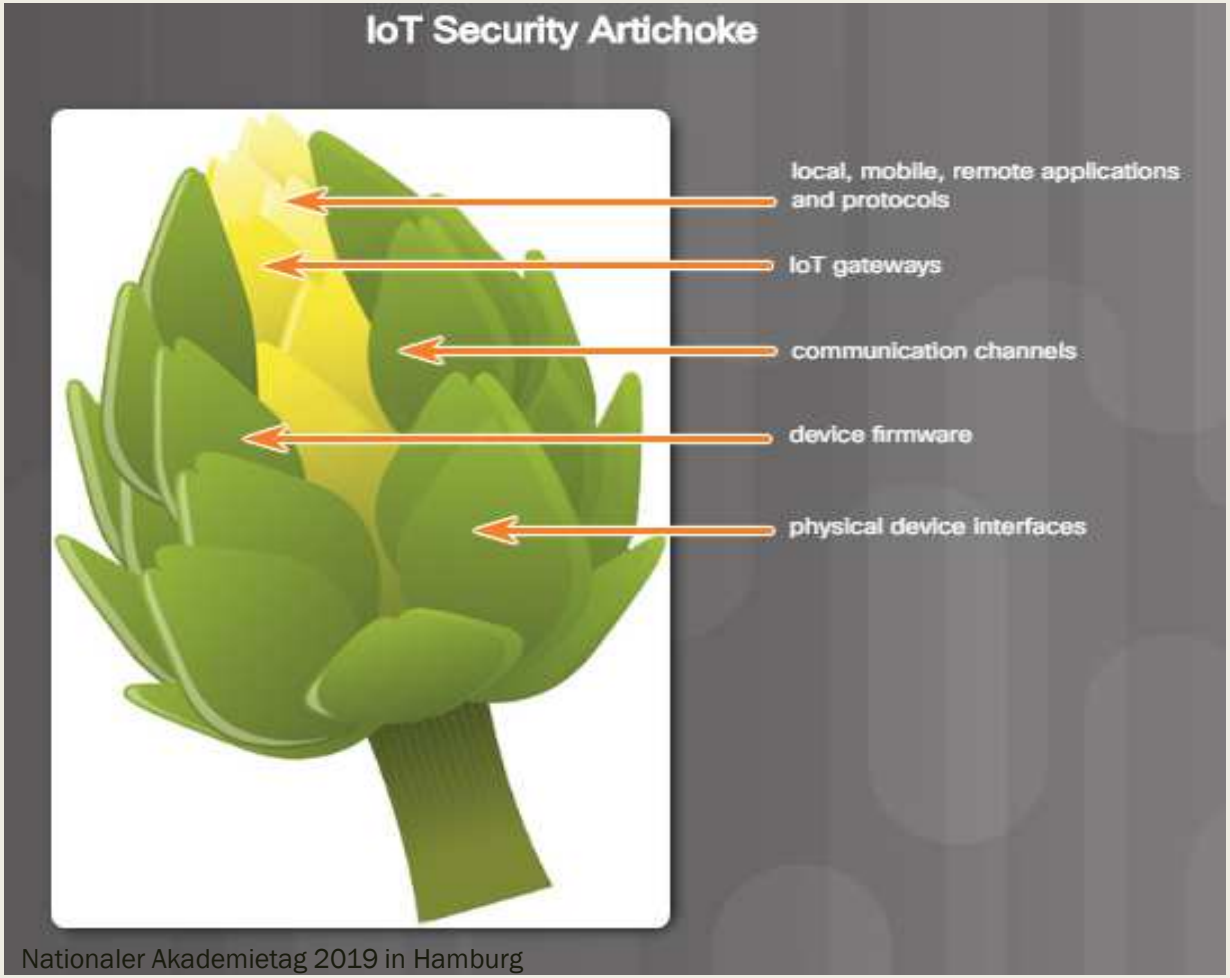
IoT Wireless Network Types

Wireless Network	Use Case
WBAN: Wireless Body Area Network	A network of wireless sensor devices that are either worn or implanted into the body. May use various wireless protocols to communicate with a gateway to post data to cloud applications.
WPAN: Wireless Personal Area Network	Frequently employs Bluetooth to connect audio devices, personal fitness trackers, and smart watches to a cell phone that serves as a gateway.
WHAN: Wireless Home Area Network	Uses Bluetooth or other wireless protocols to connect appliances, alarm system components, and actuators to gateways and the Internet.
WFAN: Wireless Field (or Factory) Area Network	Ruggedized network components connect sensors and actuators at dispersed locations in challenging manufacturing environments.
WNAN: Wireless Neighborhood Area Network	A power grid network that exists in a limited geographic area and is frequently served by a field area router that may be located outdoors.

Chapter 4: IP-Angriffsmöglichkeiten

- DoS- und DDoS-Angriffe
- Adressenfälschung in Kombination mit ICMP-Angriffe
- Man-in-the-Middle
- Syn-Flood
- Amplifikation
- Session-Hijacking

Chapter 4: allgemeine Gegenmaßnahmen



Chapter 4: Trennung von IT und OT

Netzsegmentierung, um Auswirkungen eines Angriffs zu begrenzen

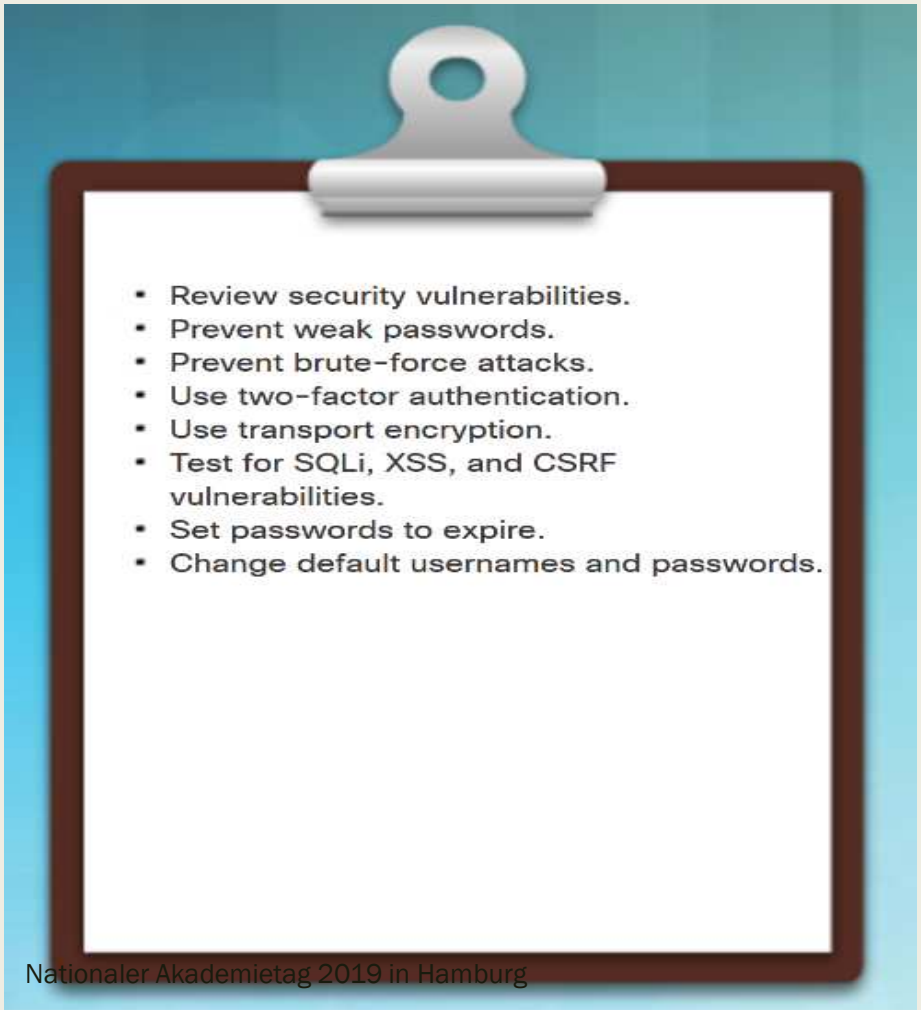
Chapter 5: Anliegen

- Feststellung von Angriffsmöglichkeiten auf IoT-Anwendungen und Protokolle
- Empfehlung von Gegenmaßnahmen

Chapter 5: Angriffsmöglichkeiten

- Allgemeine Angriffsarten auf IoT-Geräte
- Lokale Angriffe wie Ersetzung von Firmware, DoS oder Auslesen von Sicherheitseinstellungen
- Remote Angriffe wie Man-in-the-Middle, SQL-Injection und Routingangriffe
- Angriffe auf mobile Devices
- Cloud-Verwundbarkeit wie Berechtigungs- oder Authentifizierungsverletzungen

Chapter 5: Gegenmaßnahmen



Chapter 5: Bedeutung der IoT-Protokolle

- **MQTT** – Message Queueing Telemetry Transport nutzt TCP und verlangt einen Message-Broker
- **CoAP** – Constrained Application Protocol ist ein Dokumentenaustauschprotokoll, das UDP verwendet.
- **XMPP** – Extensible Messaging and Presence Protocol nutzt TCP und ist ursprünglich für Instant Messaging entworfen

- Eigenschaften:
  - Stromverbrauch
  - Bandbreite
  - Latenz
  - Sicherheit

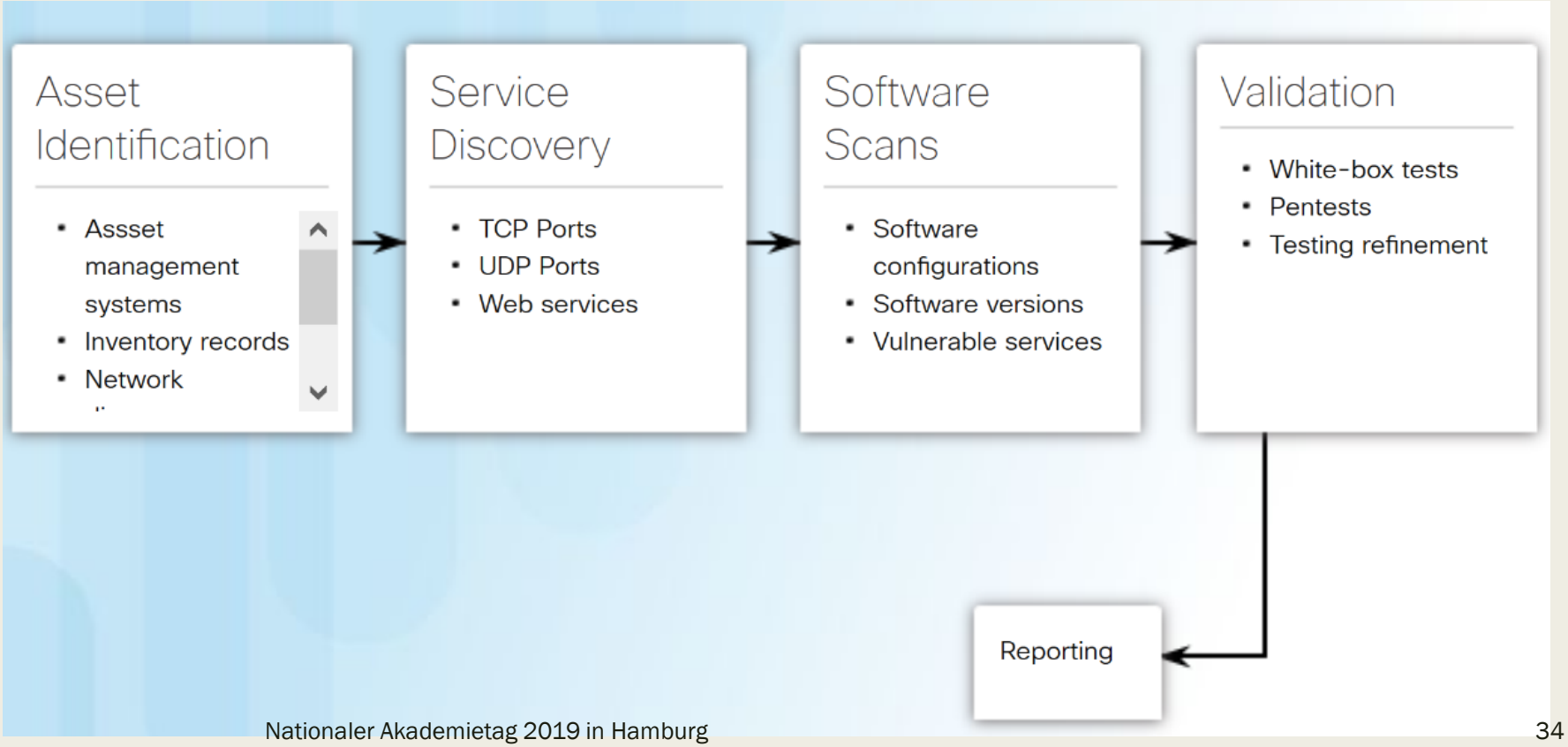
Chapter 5: Gegenmaßnahmen

- Sicherung von MQTT und CoAP durch Authentifizierung der Clients und Verschlüsselung
- Deaktivierung von UPnP (Universal Plug and Play)
- Sichere Passwortwahl
- Administrative Zugänge sichern

Chapter 6: Anliegen

- Einschätzung der Verwundbarkeit von IoT-Systemen
- Risikobewertung in IoT-Systemen

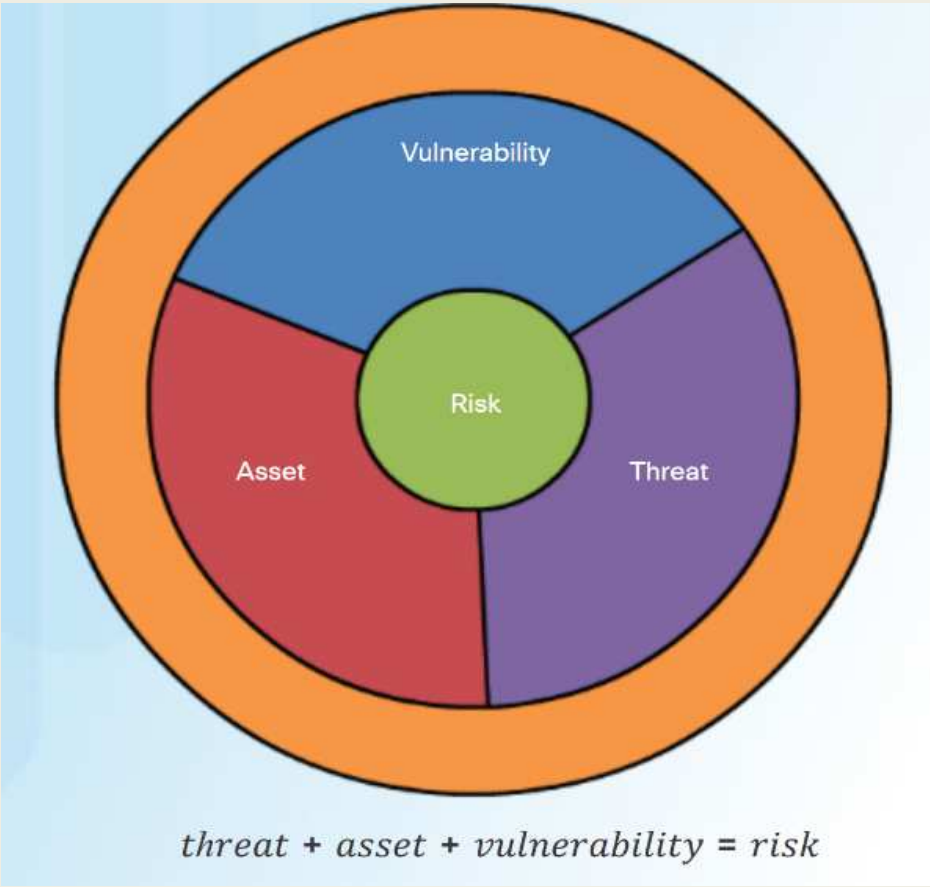
Chapter 6: Prozess zur Einschätzung der Verwundbarkeit



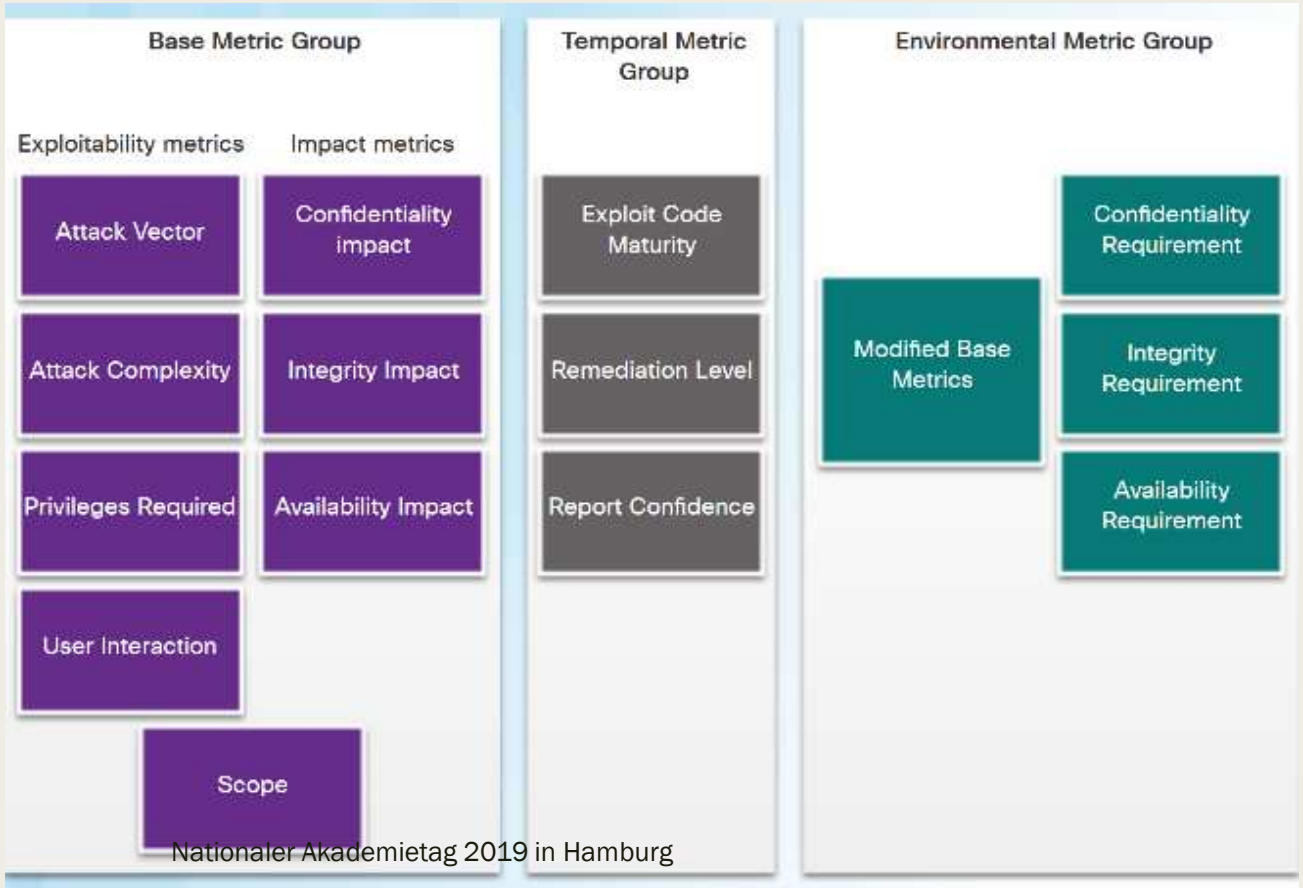
Chapter 6: Verwundbarkeitseinschätzung

- Typen
  - *White Box: der Begutachtende kennt das Netzwerk*
  - *Black Box: der Begutachtende besitzt keine Kenntnis über die Netzwerkarchitektur*
  - *Gray Box: der Prüfer verfügt über Teilkenntnisse*
- Tools:
  - *Penetration-Testing*
  - *Port-Mapping mit nmap*
  - *Web-Applikation Testing mit OpenVAS*
- Informationsquelle über Schwachstellen
  - *Common Vulnerabilities and Exposures (CVEs) Datenbank*

Chapter 6: Risikobewertung



Chapter 6: CVSS Common Vulnerability Scoring System



Chapter 6: Bedrohungsklassifikation

STRIDE Threat Classifications

Threat Classification	Definition	Example Threats
Spoofing	Impersonating a legitimate user or device	• Pretending to be a valid user or device • Pretending to be another server • Laptop impersonates IoT gateway to perform man in the middle data interception
Tampering	Modifying data, code, or device	• Modifying sensor data • Physical device hacking
Repudiation	Disabling ability to prove or disprove events	• Corrupt or destroy log files • Alter data record timestamps
Information Disclosure	Making privileged information available to unauthorized parties	• Gathering sensitive information from log files • Using SQL injection to steal personal data from web application
Denial of Service	Cause device to be unavailable to perform legitimate functions due to illegitimate traffic, data, or software	• Crashing a web site • Sending data absorbing CPU cycle, storage, or device power resources
Elevation of Privilege	Obtaining higher privileges than would normally be authorized	• Allowing remote user to run commands, switch from a limited user to admin • Using intercepted credentials to logon to data dashboard

Chapter 6: Risikobewertung

	Category	High (3)	Medium (2)	Low (1)
D	Damage potential	System down or under threat actor control; damage to people or facilities.	Loss of important data; some temporary system compromise or loss of availability.	Minor to medium loss of data or system impact.
R	Reproducibility	Every attempt will be successful.	Estimated to work half the time.	Difficult to reproduce, exploit requires special conditions.
E	Exploitability	Easily carried out by inexperienced threat actor.	Requires skilled attacker.	Requires very skilled attacker or attacking organization.
A	Affected users (or devices)	Enough devices to cause serious outages. All users who are up to standard.	Some devices that are not patched or in up to current standard.	Few users or devices under edge case configurations or roles.
D	Discoverability	Widely known in the attacker community. High value to attackers.	Little known and not widely present, some benefit to threat actors.	Little known and of little interest.

Geschafft!!

Vielen Dank für Ihre Aufmerksamkeit