# DLBCSEEIST01\_E

# Übergeordnete Lernziele

Heutzutage werden in der Welt des Internets der Dinge (IoT, Internet of Things) zahlreiche vernetzte Geräte eingesetzt, um die Lebensqualität des Einzelnen zu verbessern und von Sensoren erfasste Daten werden analysiert, um Erkenntnisse für Unternehmen und Branchen zu gewinnen. Böswillige Akteure und Hacker:innen versuchen, die Schwachstellen von IoT-Geräten und -Systemen auszunutzen, um Zugang zu wertvollen Daten zu erhalten.

Dieses Studienskript beginnt mit der Vermittlung der Grundlagen zum Thema **Internet-of-Things-Sicherheit**, indem es IoT-Architektur, Schwachstellen, Sicherheitsangriffe und Gegenmaßnahmen auf jeder Ebene von IoT-Systemen beleuchtet. Als Nächstes werden Sie mit dem Konzept der „Security by Design“ vertraut gemacht, bei dem Sicherheitsaspekte bereits in den frühen Entwicklungsphasen berücksichtigt werden. Darüber hinaus behandelt dieses Studienskript statische und dynamische Testmethoden für Anwendungen, die Code-Schwachstellen entdecken und verhindern, dass Hacker:innen diese ausnutzen.

Auch die Absicherung von End-to-End-IoT-Lösungen auf den verschiedenen Ebenen Gerät, Netzwerk und Cloud wird in diesem Studienskript untersucht. Die Sicherheitsrisiken und Konstruktionsziele von IoT-Geräten sowie die Authentifizierung und Autorisierung als zwei wichtige Konzepte der Betriebssicherheit werden erläutert. Außerdem erhalten Sie Informationen über Bedrohungen für IoT-Dienste und über die Sicherung von Cloud-Lösungen.

Abschließend werden die Konzepte von Big Data, künstlicher Intelligenz und maschinellem Lernen, einschließlich überwachter und unüberwachter Algorithmen, erörtert. Sie werden mehr über die Rolle dieser Algorithmen beim Schutz von IoT-Systemen vor Cyberkriminellen erfahren.

# Lektion 1 – Grundlagen des Internets der Dinge (IoT)

**Lernziele**

Nach dem Abschluss dieser Lektion werden Sie...

... die Hauptbestandteile der IoT-Wertschöpfungskette beschreiben können.

... die Herausforderungen bei der Einrichtung und beim Einsatz von IoT-Lösungen auflisten können.

... in der Lage sein, den architektonischen Aufbau des IoT und die Rolle der einzelnen Schichten im grundlegenden IoT-Technologiestack zu erklären.

... den Unterschied zwischen IoT für Konsumenten und industriellem IoT erklären können.

... die wichtigsten Merkmale von industriellen IoT-Anwendungen kennen.

# Grundlagen des Internets der Dinge (IoT)

## Einführung

Die Fortschritte in der Elektronik und bei den Computersystemen im späten zwanzigsten Jahrhundert ermöglichten die Maschine-zu-Maschine-Kommunikation (M2M-Kommunikation), bei der Daten und Befehle direkt (Punkt-zu-Punkt) zwischen Geräten und Maschinen übertragen werden können. Die Skalierbarkeit und das Zusammenwirken solcher hardwarebasierten M2M-Netze waren jedoch begrenzt, da alle Geräte die gleichen Kommunikationsprotokolle verwenden mussten. In der hochgradig skalierbaren Welt des Internets der Dinge (IoT) kann jedoch so gut wie jedes „Ding“ – von einem einfachen Lichtsensor oder einem intelligenten Toaster bis hin zu sehr fortschrittlichen Robotern in intelligenten Fabriken – mit dem Internet verbunden werden und darüber mit anderen intelligenten Geräten und Nutzenden in der Welt kommunizieren.

## Einführung in das IoT

Spezielle Kommunikationstechnologien wie **Low-Power-Wide-Area-Networks** (LPWAN) ermöglichen viele IoT-Einsatzfälle, indem sie den intelligenten Geräten ermöglichen, monatelang mit kleinen Batterien zu arbeiten, so dass sie Daten mit der Cloud und anderen IoT-Geräten austauschen können, ohne dass eine regelmäßige Wartung oder ein Batteriewechsel erforderlich ist. Die IoT-Geräte mit begrenzten Ressourcen im LPWAN sind am anfälligsten für Sicherheitsbedrohungen, da Cyber-Angreifende sich in der Regel auf die schwächste Komponente der Infrastruktur konzentrieren – bei der es sich um solche kostengünstigen Geräte handeln kann.

Darüber hinaus sind leistungsstarke Datenanalysetools in der Lage, die riesigen Datenmengen zu analysieren, die von den zahlreichen IoT-Geräten in Smart Homes, intelligenten Fabriken, intelligenten Stromnetzen, Wearables usw. empfangen werden, und daraus Erkenntnisse für Einzelpersonen, Unternehmen und Organisationen zu gewinnen.

**Low-power Wide-area (LPWA)**

Eine Gruppe zellularer und nicht zellularer Kommunikationstechnologien mit geringer Leistung und großer Reichweite, die in vielen IoT-Anwendungen eingesetzt werden.

IoT-Einsatzfälle verbinden viele Dinge miteinander und bringen viele Vorteile für Einzelpersonen, Unternehmen und Gesellschaften durch ein Ökosystem mit vier Hauptelementen, die zusammenarbeiten, um die Ziele einer vernetzten Welt zu erreichen: Dinge, Menschen (Entwickelnde, Netzbetreiber und Nutzende), Daten (Informationen, die von Sensoren erfasst und an die Cloud übertragen werden, sowie Befehle an das intelligente Objekt) und Prozesse (Farshad Firouzi, 2020). Im Konzept des IoT muss ein Gerät oder Ding die folgenden vier Merkmale aufweisen, um als IoT-Gerät oder intelligentes Objekt zu gelten (David Hanes, 2017):

1. Sensor(en) und Aktor(en) zur Interaktion mit der physischen Welt.
2. Eine Kommunikationseinheit zur Verbindung des intelligenten Objekts mit dem Internet.
3. Stromquelle zur Versorgung der Sensoren, Kommunikations- und Verarbeitungssysteme.
4. Verarbeitungseinheit zur Verarbeitung und Analyse der von den Sensoren gesammelten Daten und zur Steuerung anderer Systeme wie Energie- und Kommunikationseinheiten.

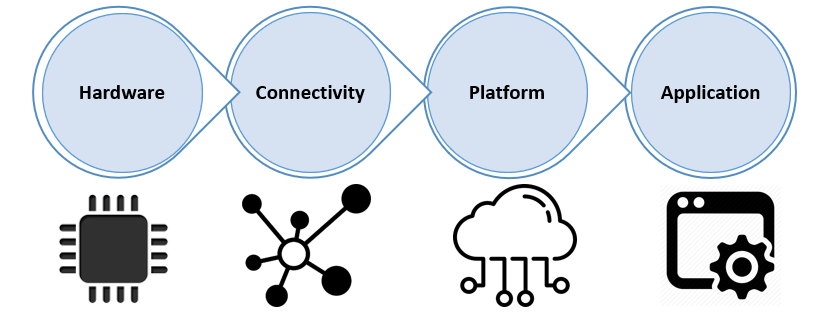
### Auswirkungen des IoT

In naher Zukunft wird sich das IoT auf jeden Aspekt unseres Lebens auswirken, sei es auf die Art und Weise, wie wir unsere Gesundheit überwachen, wie wir zur Arbeit kommen oder wie wir unsere Einkäufe erledigen. Auch für Organisationen und Unternehmen bringt es viele Vorteile mit sich. Die sich aus der Analyse der IoT-Daten ergebenden Maßnahmen und Ergebnisse können die Produktivität durch eine effektivere Verwaltung der Ressourcen steigern. Das IoT schafft Transparenz, indem es den Standort von Vermögenswerten und den Status von Prozessen, wie z. B. Produktionslinien, identifiziert. Die IoT-Rule-Engines in Verbindung mit künstlicher Intelligenz (KI) automatisieren und erhöhen die Genauigkeit von Prozessen und sagen Ausfälle in Systemen voraus, um Probleme zu vermeiden. Darüber hinaus kann das IoT bei der Bewältigung von Sicherheitsproblemen helfen, indem es gefährliche Situationen und Umgebungsfaktoren zuverlässiger und schneller erkennt (Farshad Firouzi, 2020).

### IoT-Wertschöpfungskette

Jede IoT-Lösung besteht aus verschiedenen Komponenten und Bausteinen, die von einer Reihe von Unternehmen entwickelt werden. Diese Komponenten werden als IoT-Wertschöpfungskette bezeichnet und spielen verschiedene Rollen, die den Endnutzenden der Lösung einen gewissen Mehrwert bieten. Zu den Komponenten einer IoT-Wertschöpfungskette gehören Hardware, Konnektivität, Plattform und Anwendung (Rebbeck, 2020).

Die IoT-Wertschöpfungskette



Quelle: Reza Vahidnia (2022)

Die Hardware umfasst eine Reihe von Sensoren/Aktoren, die Daten erfassen/verarbeiten, sowie die für die Kommunikation verwendete Hardware (d. h. Chipsätze und SIM-Karten für die Verbindung des Geräts mit dem Netzwerk). Die Konnektivitätskomponente (z. B. ein Mobilfunknetzbetreiber) ist für die Übertragung der Daten und Befehle zwischen den Sensoren/Aktoren und dem Backend (d. h. den Servern, die Daten sammeln) zuständig. Die IoT-Plattform (z. B. ThingsBoard, Microsoft Azure oder Amazon Web Services) gilt als zentrales Rückgrat des IoT und dient dazu, die Lücke zwischen Hardware und Anwendungen zu schließen, indem sie Entwickelnde eine Kombination gebrauchsfertiger Funktionen zur Verfügung stellt. Das Anwendungselement ist der Bereich, in dem die Entwickelnden ihren Anteil am IoT erhöhen, indem sie nützliche Schnittstellen für die Nutzenden schaffen.

### IoT-Cluster

Das IoT kann in verschiedene Cluster eingeteilt werden, und zwar in Branchen, Einsatzfälle und Anwendungen. Diese Cluster werden in der Abbildung unten dargestellt.

IoT-Cluster

Quelle: Reza Vahidnia (2022)

Verschiedene IoT-Einsatzfälle haben unterschiedliche Vorteile für verschiedene Branchen und Segmente. Die zu einem bestimmten Branchensegment gehörenden IoT-Einsatzfälle werden einem IoT-Vertical mit eigenen Regulierungsstellen, Verfahren, Protokollen und Normierungsorganisationen zugeordnet (Dian & Vahidnia, 2021). Diese IoT-Einsatzfälle erfordern in der Regel ähnliche Datenspeicher-, Datenverarbeitungs- und Analysefähigkeiten. Die IoT-Einsatzfälle „intelligenter Kühlschrank“ und „intelligente Waschmaschine“ gehören beispielsweise beide zum Vertical „Smart Home“ und dienen dem Komfort der Hausbewohnenden und der Energieeinsparung. Ein weiteres Beispiel ist die „intelligente Fabrik“, die als IoT-Einsatzfall zur Verringerung menschlicher Fehler und der Betriebskosten in der Industrie angesehen wird.

Jeder IoT-Einsatzfall kann mehrere IoT-Anwendungen umfassen, die ähnliche Lösungen und Software verwenden. Beispielsweise können in dem Einsatzfall „vernetztes Fahrzeug“ Anwendungen für Infotainment, Telematik und Flottenmanagement genutzt werden.

### Herausforderungen für das IoT

Neben den zahlreichen Vorteilen bringen die Einführung und der Einsatz von IoT-Lösungen auch ihre eigenen Herausforderungen mit sich. Dazu gehören:

* **Skalierbarkeit:** Eine enorme Anzahl von IoT-Geräten (bis zu mehreren Millionen Sensoren) muss an das Netz angeschlossen werden. Aus diesem Grund ist IPv4 für den Aufbau von IoT-Netzen möglicherweise nicht ausreichend.
* **Interoperabilität:** IoT-Geräte gibt es von verschiedenen Anbietern, mit unterschiedlichen Normen und Kommunikationsprotokollen. Die Entwicklung eines Netzwerks, das all diese verschiedenen Normen und Protokolle unterstützt, könnte daher eine Herausforderung darstellen.
* **Sicherheit:** Vertrauliche Daten, die von IoT-Sensoren erfasst werden, müssen sicher geschützt werden, wenn sie vom Sensor erzeugt, von Edge-Geräten verarbeitet, an die Cloud übertragen, in der Datenbank gespeichert, von Menschen, Anwendungen und anderen Diensten abgerufen und von Analysesoftware analysiert werden.
* **Datenschutz:** Privatpersonen und Unternehmen wollen wissen, ob und an wen die gesammelten Daten weitergegeben werden. Aus diesem Grund zögern manche Menschen, IoT-Geräte in ihrem täglichen Leben oder in ihren Unternehmen einzusetzen.
* **Big Data und Analytik:** Die diversen Arten von Daten, die von verschiedenen Sensoren erfasst werden, müssen richtig aufbereitet und strukturiert werden, bevor sie gespeichert, analysiert und dargestellt werden können.
* **Rechtliches:** Das geistige Eigentum und die Haftung jedes Akteurs im Ökosystem sollten klar definiert sein.
* **Begrenzte Ressourcen:** Die meisten IoT-Geräte sind einfach und kostengünstig und verfügen nur über begrenzte Speicher-, Leistungs- und Verarbeitungskapazitäten. Daher kann die Implementierung starker Sicherheitsmechanismen auf IoT-Geräten schwierig oder unmöglich sein.

### Fragen zur Selbstkontrolle

1. Bitte nennen Sie die vier Hauptkomponenten der IoT-Wertschöpfungskette.

*Hardware*

*Konnektivität*

*Plattform*

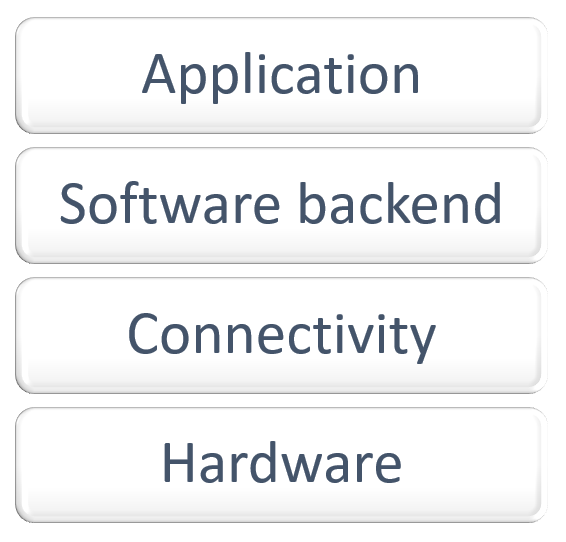
*Anwendungen*

## 1.2 Architektur

Wie Bauprojekte, die eine sorgfältige Planung und eine Architektur erfordern, die bestimmte Normen einhält, sollten auch IoT-Netzwerke sorgfältig geplant und unter Einhaltung bewährter Designpraktiken und Sicherheitsrichtlinien aufgebaut werden. Andernfalls wird es äußerst schwierig, die IoT-Netze zu verwalten, zu skalieren, anzupassen und Fehler zu beheben (David Hanes, 2017).

Eine solide IoT-Infrastruktur und ein architektonisches Modell sind notwendig, um IoT-Lösungen zu entwickeln und die riesigen Datenmengen zu bewältigen, die von der großen Anzahl intelligenter Geräte erzeugt werden. Aus Sicht der Netzwerkarchitektur besteht der vereinfachte IoT-Technologiestack aus vier Hauptschichten, wie in der folgenden Abbildung dargestellt. In jeder dieser vier Schichten des IoT-Technologiestacks wird Sicherheit als ein wesentliches Element betrachtet (Vahidnia & Dian, 2021).

Grundlegender IoT-Technologiestack



Quelle: Reza Vahidnia (2022)

### Hardware

Die Hardware-Schicht oder Schicht der Dinge ist der Ort, an dem von IoT-Sensoren Daten erzeugt werden. Diese Schicht umfasst die intelligenten Geräte (Dinge) mit eingebauten Sensoren zur Messung physikalischer Parameter, Aktoren zur Ausführung physikalischer Aufgaben, einen kostengünstigen Mikroprozessor oder Mikrocontroller, eine Energiequelle (z. B. Batterie, Netz, Solar) und ein Kommunikationsmodul zum Senden von Sensordaten und zum Empfangen von Anweisungen und Befehlen.

Die Betrachtung der Hardware- oder Dingebene ist der erste Schritt bei der Entwicklung einer IoT-Lösung. Die Eigenschaften und die Art der intelligenten Sensoren in dieser Schicht sowie die Anforderungen des IoT-Einsatzfalls bestimmen die Technologien und Protokolle, die in den oberen Schichten des IoT-Technologiestacks verwendet werden sollten. Intelligente Sensoren, die mit Batterien betrieben werden, sind in der Regel sehr mobil und benötigen daher für ihre Kommunikation drahtlose Technologien mit minimalem Stromverbrauch (z. B. LPWA).

IoT-Architekt:innen sollten bei der Wahl der richtigen IoT-Zugangstechnologie auch besonders auf die Übertragungsreichweite und Meldefrequenz der Sensoren achten. Mit dem Stromnetz verbundene Sensoren wie intelligente Zähler sind in der Regel statisch und können daher Technologien und Protokolle mit höherem Stromverbrauch verwenden, die ihnen größere Übertragungsreichweiten ermöglichen, und ihre Daten häufiger melden.

Der Stromverbrauch der IoT-Geräte hängt erheblich davon ab, ob die von den intelligenten Sensoren erzeugten Daten umfangreich oder einfach sind und welche Zeitspannen zwischen aufeinanderfolgenden Berichten liegen. Darüber hinaus können die Kommunikationstechnologie und die Anwendungsprotokolle, die von IoT-Geräten zum Datenaustausch mit der Cloud verwendet werden, den Stromverbrauch des IoT-Systems bestimmen. Wenn die IoT-Daten, die von den in einer Verbindung installierten Sensoren erzeugt werden, sehr umfangreich sind, wird mehr Energie für die Verarbeitung und Übertragung benötigt. Wenig Energie und ein geringer Datendurchsatz (Datenrate) wird beispielsweise für einen Feuchtigkeitssensor benötigt, der nur einfache Daten zur Übertragung in die Cloud erzeugt.

Die Reichweite eines intelligenten Geräts bzw. die Entfernung, über die der Sensor seine erfassten Daten senden muss, ist ein weiteres wichtiges Merkmal eines IoT-Geräts. So kommuniziert beispielsweise ein in einem Fluss installierter Wasserqualitätssensor mit einem einige Kilometer entfernten Funkturm eines Mobilfunkbetreibers. Für solche IoT-Einsatzfälle und -Anwendungen mit großen Reichweiten wird eine LPWA-Kommunikationstechnologie benötigt, um die IoT-Geräte in einem großen Bereich abzudecken.

Die obigen Einsatzfälle zeigen, dass für die Entwicklung einer IoT-Initiative zunächst die Anforderungen der IoT-Sensoren in Bezug auf den Stromverbrauch (batteriebetrieben oder mit Stromanschluss), die Entfernung zum Gateway, die Mobilität (z. B. stationär oder mobil in einem kleinen oder großen Gebiet), die Zeitspanne zwischen zwei aufeinanderfolgenden Datenübertragungen und der Durchsatz (Datenübertragungsrate) untersucht werden müssen (Vahidnia & Dian, 2021).

Auf der Hardware-Ebene können Cyber-Angreifende versuchen, die IoT-Geräte zu kompromittieren, indem sie die Sensoren/Aktoren manipulieren oder physisch beschädigen, böswillige Netzknoten einschleusen, um die übertragenen Daten zu verändern, die Funksignale stören, um die Kommunikation zwischen den IoT-Geräten zu unterbrechen, oder den Stromverbrauch der IoT-Geräte erhöhen. Eine Möglichkeit zur Lösung der Sicherheitsprobleme auf dieser Ebene besteht darin, zu gewährleisten, dass alle IoT-Geräte ordnungsgemäß authentifiziert werden, bevor sie mit dem Rest des IoT-Systems kommunizieren können.

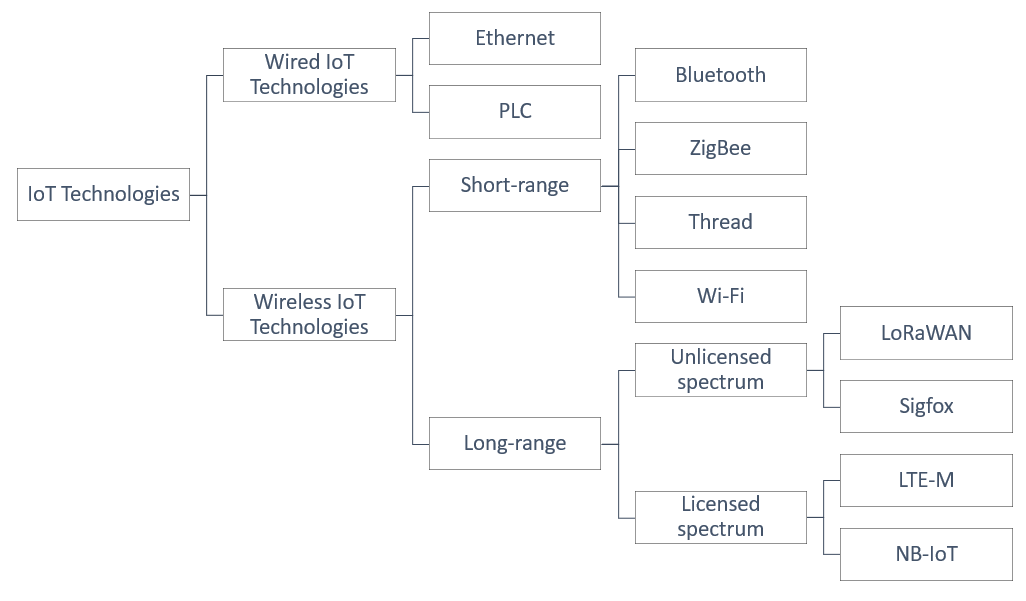
### Konnektivität

Die Kommunikations- oder Konnektivitätsschicht ermöglicht die Verbindung zwischen den IoT-Geräten (Hardware) und dem Internet über eine IoT-Zugangstechnologie wie Wi-Fi, Bluetooth oder Mobilfunk. Die Kommunikationsschicht transportiert die Daten/Befehle von den Sensoren/Aktoren zum/vom Netz über verschiedene Zugangstechnologien, die sich in Bezug auf Architektur, Stromverbrauch, Reichweite, Datenübertragungsrate und Sicherheitsanforderungen grundlegend unterscheiden.

In dieser Schicht können Cyber-Angreifende versuchen, die IoT-Daten abzufangen und abzuhören, den IoT-Verkehr auf einen kompromittierten Netznoten zu lenken oder einen einzelnen Netzknoten mit mehreren gefälschten Identitäten zu betreiben. Dies ist ein effizientes Verfahren zum Schutz vertraulicher Informationen während der Übertragung zwischen IoT-Objekten ist die Kryptografie. Dabei kommen verschiedene Algorithmen zur Anwendung, die Chiffren genannt werden. Diese verschlüsseln die Klartextdaten, indem sie eine Zahlenreihe als Schlüssel verwenden, um einen Chiffretext zu erstellen. Die Chiffrierschlüssel können entweder symmetrisch (derselbe Schlüssel wird sowohl für die Ver- als auch für die Entschlüsselung verwendet) oder asymmetrisch sein, d. h. es werden zwei verschiedene Schlüssel für die Ver- und Entschlüsselung der Daten verwendet.

In den meisten IoT-Einsatzfällen verwenden die intelligenten Geräte eine der in der folgenden Abbildung dargestellten Kommunikationstechnologien, um mit dem Software-Backend (Cloud-Dienst) zu kommunizieren, in dem die Daten und alle angeschlossenen Geräte verwaltet werden.

IoT-Zugangstechnologien



Quelle: Reza Vahidnia (2022)

Je nach IoT-Einsatzfall und Mobilität der intelligenten Sensoren kann die Zugangstechnologie kabelgebunden oder drahtlos sein. Kabelgebundene Zugangstechnologien wie Ethernet unterstützen in der Regel höhere Datenraten und gelten im Vergleich zu drahtlosen Netzen als zuverlässiger und sicherer. Auf der anderen Seite sind kabelgebundene Netze aufgrund der Kosten für die Verkabelung teurer und es fehlt ihnen an Mobilität und Skalierbarkeit. Die beiden wichtigsten kabelgebundenen Technologien, die in IoT-Netzwerken verwendet werden, sind Ethernet und Power Line Communication (PLC). Ethernet ist die am häufigsten verwendete LAN-Technologie (Local Area Network), die Datenübertragungsraten von bis zu einigen Gigabit pro Sekunde unterstützen kann. PLC nutzt die normalen Stromleitungen für Datenübertragungen von bis zu einigen hundert Kilobit pro Sekunde.

Im Vergleich dazu sind drahtlose Netze leicht erweiterbar und wesentlich kostengünstiger als kabelgebundene Technologien (einfache Installation). Zu den weit verbreiteten drahtlosen Technologien für die Nahbereichs-Kommunikation gehören Zigbee, Z-Wave, Wi-Fi und Bluetooth.

Technologien für die Kommunikation über große Entfernungen sind entweder lizenziert (z. B. LTE-M und NB-IoT) oder nicht lizenziert (z. B. LoRa und Sigfox). Diese Technologien ermöglichen eine flächendeckende Versorgung mit geringem Stromverbrauch (Low Power Wide Area; LPWA), wie sie für die meisten drahtlosen Sensornetzwerke erforderlich ist. Die Frequenzen und die Sicherheit der lizenzierten LPWA-Technologien werden von den Netzbetreibern garantiert, während es für nicht lizenzierte Kommunikationstechnologien keine solchen Frequenzgarantien gibt.

### Software-Backend

Das Software-Backend umfasst die in der Cloud laufenden Dienste, welche die IoT-Sensoren/Aktoren sowie das Netzwerk verwalten. Diese Cloud-Dienste bieten auch Schnittstellen zur Verknüpfung des IoT mit Drittsystemen wie Customer Relationship Management (CRM, Kundenbeziehungsmanagement) und Enterprise Resource Planning (ERP, Unternehmensressourcenplanung). Ein Hauptbestandteil des zentralen Software-Backends ist die IoT-Plattform. Microsoft Azure, ThingsBoard, IBM Watson und GE Predix sind einige der bekannten und führenden IoT-Plattformen. Ihre Aufgaben sind die Verarbeitung der Ereignisse, die Verwaltung der Geräte und Aktionen, die Bereitstellung fortschrittlicher Analysen, die Bereitstellung von Datenbanken zur Datenspeicherung und die Integration der IoT-Systeme mit den externen Schnittstellen und APIs (Application Programming Interfaces, Programmierschnittstellen).

### Anwendung

Die Anwendungsschicht ist dafür verantwortlich, die von den IoT-Sensoren empfangenen Daten in Echtzeit zu visualisieren und die Zusammenarbeit zwischen verschiedenen Unternehmen und Organisationen zu ermöglichen. Im Grunde genommen verwandelt diese Schicht die von den IoT-Geräten gesammelten IoT-Rohdaten in Nutzwerte für Einzelpersonen, Unternehmen und Organisationen. Außerdem steuern die von der Anwendungsschicht gesendeten Befehle das Verhalten der IoT-Geräte.

In dieser Schicht können sowohl die Daten als auch das Netz analysiert werden. Die Datenanalyse interpretiert die IoT-Daten und schafft Einblicke in den Einsatzfall, indem sie die von den IoT-Geräten erzeugten Daten verarbeitet und analysiert. Die Netzwerkanalyse wird in der Regel in unternehmenskritischen Einsatzfällen, wie z. B. der Steuerung von Drohnen durchgeführt, um sicherzustellen, dass das Netzwerk betriebsbereit ist und die Anforderungen an Latenz und Zuverlässigkeit erfüllt. Da eine detaillierte Analyse des Netzwerks in Echtzeit sehr teuer sein kann, bestimmen IoT-Architekt:innen die Tiefe der Netzwerkanalyse auf der Grundlage der Anwendbarkeit der IoT-Lösung. In Einsatzfällen wie der Temperatur- oder Luftfeuchtigkeitsüberwachung, bei denen lange Zeiträume zwischen aufeinanderfolgenden IoT-Datenmeldungen an die Cloud liegen, genügt eine einfache Netzwerkanalyse, um die Betriebsbereitschaft des Netzwerks sicherzustellen. Andererseits ist in industriellen IoT-Netzen oder unternehmenskritischen Anwendungen eine tiefgreifende Netzanalyse erforderlich (Vahidnia & Dian, 2021).

### Fragen zur Selbstkontrolle

1. Nennen Sie bitte die beiden komplementären lizenzierten Schmalbandtechnologien, die für die Kommunikation mit großer Reichweite zwischen IoT-Geräten verwendet werden.

LTE-M

NB-IoT

1. Bitte erklären Sie die Rolle des Software-Backends im grundlegenden IoT-Technologiestack.

Das Software-Backend umfasst die in der Cloud laufenden Dienste, welche die IoT-Sensoren/Aktoren sowie das Netzwerk verwalten. Diese Cloud-Dienste bieten auch Schnittstellen zur Verknüpfung des IoT mit Drittsystemen. Wichtige Aufgaben des zentralen Software-Backends sind die Verarbeitung der Ereignisse, die Verwaltung der Geräte und Aktionen, die Bereitstellung fortschrittlicher Analysen, die Bereitstellung von Datenbanken zur Datenspeicherung und die Integration der IoT-Systeme mit den externen Schnittstellen und APIs.

1. Bitte wählen Sie aus, welche Schicht im IoT-Technologiestack die Art der Kommunikationstechnologie bestimmt, die zur Übertragung der Daten von den Sensoren an die Cloud verwendet wird.

* Konnektivität
* Anwendung
* *Hardware*
* Anwendung

## 1.3 Nicht-industrielles Internet der Dinge

Das nicht-industrielle oder Verbraucher-IoT ist die Einbindung von IoT in normale Verbraucheranwendungen und -geräte. Es handelt sich dabei um ein Netz intelligenter Sensoren, wie z. B. an Wearables, die mit verschiedenen IoT-Zugangstechnologien betrieben werden, um den Verbraucher:innen durch die Automatisierung ihrer täglichen Aufgaben Komfort zu bieten. Im Vergleich zu industriellen IoT-Geräten sind Verbraucher-IoT-Geräte in der Regel kostengünstiger und weisen ein geringeres Maß an Robustheit, Sicherheit, Skalierbarkeit und Langlebigkeit des Netzwerks auf.

Die wichtigsten Anwendungen des nicht-industriellen IoT reichen von sehr einfachen Geräten zur Überwachung der persönlichen Fitness bis hin zu fortschrittlichen Smart Homes. Nicht-industrielle IoT-Anwendungen und Einsatzfälle werden hauptsächlich in zwei Kategorien unterteilt:

* Personengebundene IoT-Anwendungen und -Geräte, zu denen Wearables (z. B. intelligente Kleidung, intelligente Uhren, intelligente Brillen), Hearables (z. B. AirPods), Smartphones und persönliche Laptop-Gadgets gehören.
* Smart Home IoT-Anwendungen und -Geräte, einschließlich Energiespar- und Hausautomatisierungsprodukte (z. B. Philips Hue-Glühbirnen) und Sicherheitssysteme mit Sprachsteuerung (z. B. Amazon Echo) und Gesichtserkennung usw.

Bis 2026 wird der Verbraucher-IoT-Markt laut einem IoT-Marktbericht von Global Consumer 153,80 Milliarden $ (142 Mrd. €) wert sein (iot-consumer-applications, 2022). Geräte für die Hausautomatisierung mit Funktionen für Sicherheit, Fernverwaltung und intelligente Energieversorgung werden den IoT-Markt bis 2023 dominieren. Im Folgenden werden einige der wichtigsten Einsatzfälle des nicht-industriellen (Verbraucher-)IoT genannt (iot-consumer-applications, 2022):

### Sicherheit und Schutz des Hauses

In Smart Homes kann das IoT Aufgaben automatisieren und den Energieverbrauch senken. IoT-Sensoren können zum Beispiel Ankunftszeiten der Bewohnenden erfassen, um die Temperatur und die Beleuchtung des Hauses entsprechend einzustellen. Intelligente Sensoren verfolgen ständig Bewegungen, um die Sicherheit des Hauses zu erhöhen und die Sicherheit von Kindern und älteren Menschen im Haus zu verbessern.

### Arbeits- und Büroumgebung

Der Einsatz von IoT-Geräten am Arbeitsplatz kann Kosten und Zeitaufwand der Mitarbeitenden senken. IoT-Geräte und -Aktoren bereiten beispielsweise den Präsentationsraum vor und zeichnen die Sitzungen auf, erstellen Protokolle und senden sie automatisch an die Teilnehmer:innen. Durch die Analyse von IoT-Daten können Einblicke in das Unternehmenswachstum gewonnen und künftige Markttrends vorhergesehen werden, um die Produktivität des Unternehmens zu steigern.

### Unterhaltung und Lifestyle

Das Internet der Dinge kann in der Unterhaltungs- und Tourismusbranche einen Wendepunkt darstellen. Tourist:innen können sich in Städten von IoT-Geräten zu Orten ihres Interesses führen lassen. Urlaube können durch Analyse von IoT-Daten effektiver geplant werden, wobei Reisenden je nach Budget und Interesse die besten Optionen (z. B. Buchung von Hotelzimmern und Eintrittskarten für Sehenswürdigkeiten) vorgeschlagen werden können.

### Persönliche Assistenten

IoT-Geräte wie Alexa von Amazon, Google Assistant oder Siri können ihre Befehle über die menschliche Stimme erhalten und die notwendigen Aktionen ausführen, z. B. Musik abspielen, ein Kochrezept oder die Wettervorhersage mitteilen oder einen Timer einstellen.

### Smart Wearables

Intelligente Wearables wie Smartwatches, intelligente Gürtel oder intelligente Ohrhörer können als Accessoire getragen oder als Tätowierung in den Körper eingepflanzt werden und dienen der Überwachung der Gesundheit (z. B. des Pulses) und der täglichen Aktivität (Aufzeichnung der Anzahl der Schritte) der Nutzenden.

### Nachverfolgung von Vermögensgegenständen

Vermögensgegenstände wie Haustiere, Fahrzeuge und Pakete können mithilfe von IoT-Sensoren ständig verfolgt und überwacht werden.

### Pflege älterer Menschen

Der Gesundheitszustand älterer Menschen kann mithilfe von Überwachungstechnologien wie Bewegungssensoren und Mikrofonen aus der Ferne beobachtet werden. IoT-Systeme können auch den Blutzuckerspiegel von Pflegebedürftigen überprüfen und die Ergebnisse im Notfall an den Gesundheitsdienstleister melden. Die aufgezeichneten Ergebnisse können auch gespeichert und für spätere Zwecke analysiert werden, so dass Patient:innen nicht bei jedem Arztbesuch Formulare ausfüllen müssen.

### Fragen zur Selbstkontrolle

1. Bitte nennen Sie vier Haupteinsatzfälle des nicht-industriellen IoT.

*Sicherheit und Schutz des Hauses*

*Arbeits- und Büroumgebung*

*Unterhaltung und Lifestyle*

*Persönliche Assistenten*

## 1.4 Industrie 4.0 (industrielles IoT)

Industrielles IoT oder IIoT bezieht sich auf die Anwendung von IoT-Technologien wie Machine-to-Machine-Kommunikation (M2M-Kommunikation), Big Data und maschinellem Lernen zur Optimierung industrieller Abläufe und zur Verbesserung der Effizienz in verschiedenen Industriesektoren. Das IIoT besteht aus einem Netzwerk von IoT-Sensoren, die mit einer **speicherprogrammierbaren Steuerung (SPS)** verbunden sind, in der die erzeugten Sensordaten mithilfe von Cloud-basierten Lösungen verarbeitet werden, um den Betrieb zu optimieren. Cyber-Angreifende können es auf SPS abgesehen haben, die Maschinen in kritischen Infrastrukturen steuern. Ein erfolgreicher Angriff auf eine SPS ermöglicht böswilligen Personen

**Speicherprogrammierbare Steuerung (SPS)**

Ein robuster industrieller Computer zur Steuerung von Fertigungsprozessen.

* Alarmschwellen zu ändern oder zu deaktivieren.
* den Betrieb der Anlage zu stören.
* sensible Informationen zu stehlen.
* falsche Daten an Systembetreiber zu senden, um diese zu unangemessenen Aktionen zu veranlassen.
* den Datenfluss zu blockieren oder zu verzögern.

IIoT-Ökosysteme verändern Unternehmen auf ihrem Weg zur [Industrie 4.0 maßgeblich. Industrie 4.0 ist die vierte industrielle Revolution, bei der intelligente, mit Sensoren ausgestattete Maschinen miteinander kommunizieren und vernetzte Fabriken bilden. In solchen intelligenten Fabriken werden Entscheidungen mit Hilfe von IoT getroffen, Ausfälle von Anlagen und Prozessen werden vorhergesagt, und die Maschinen verfügen über Selbstheilungsfunktionen, um menschliche Eingriffe zu minimieren. Nachfolgend werden die wichtigsten Merkmale des industriellen IoT erläutert (guide-on-industrial-vs-consumer-iot, 2022).](https://www.intuz.com/blog/things-to-know-about-industry-4-0)

### Widerstandsfähigkeit gegen extreme Umgebungsbedingungen

Industrielle IoT-Sensoren sind so konzipiert, dass sie extremen Umgebungsbedingungen wie hohen Temperaturen und hoher Luftfeuchtigkeit standhalten, in Flüssigkeiten eingetaucht und bei hohem Druck eingesetzt werden können. Diese Sensoren erfüllen auch die Anforderungen an die Wasserdichtigkeit gemäß der IP68-Zertifizierung.

### Breite Gerätepalette

**Supervisory Control and Data Acquisition (SCADA)**

Eine Architektur von Steuerungssystemen, die für die High-Level-Überwachung von industriellen Prozessen und Maschinen verwendet werden.

Industrielle Überwachungssysteme werden in der Regel in großen Anlagen und Arealen eingesetzt. Daher müssen IoT-Geräte ihre Daten über eine große Entfernung an die industriellen Kontrollsysteme wie SPS oder **Supervisory Control and Data Acquisition (SCADA)** übertragen. Um eine Überlastung der industriellen Kontrollsysteme (ICS) zu vermeiden, wird die Vorabanalyse in der Regel auf der Geräteebene (Edge Computing) durchgeführt.

### Maximale Kommunikation

In einigen Branchen wie Bergbau, Forstwirtschaft, Öl und Gas werden die industriellen IoT-Sensoren in der Regel an schwer zugänglichen Orten installiert und müssen daher über spezielle industrielle Batterie- und Kommunikationsfunktionen verfügen. Low-Power-Wide-Area-Technologien (LPWA) wie Narrow-Band-IoT (NB-IoT) und LoRaWAN ermöglichen es den IoT-Geräten, über einen längeren Zeitraum (sogar bis zu zehn Jahre) mit einer einzigen Batterie zu arbeiten, ohne dass diese ausgetauscht werden muss.

### Höhere Cybersicherheitsstandards

Industriegeräte und -netze sind anfälliger für Sicherheitsbedrohungen und erfordern strengere Cybersicherheitsprotokolle bei der Installation der Hardware oder dem Datenaustausch mit der Cloud.

Um Branchen und Unternehmen bei der Sicherung ihrer IIoT-Systeme zu unterstützen, empfiehlt Amazon Web Services (AWS) einen mehrschichtigen Ansatz mit folgenden Regeln (Dsouza, 2021):

1. Risikobewertung für die Cybersicherheit durchführen.
2. Netzwerkarchitektur und den Bestand an IoT-Geräten auf dem neuesten Stand halten.
3. Zugangskontroll- und Authentifizierungsverfahren anwenden und IIoT-Geräte mit eindeutigen Referenzen und Identitäten ausstatten.
4. Bereitstellung geeigneter Firmware-Update-Mechanismen für IIoT-Geräte.
5. Verschlüsselung der Edge- und Cloud-Daten im Ruhezustand und Sicherung der Datenverwaltung und -freigabe.
6. Umwandlung der unsicheren Industrieprotokolle in sichere und standardisierte Protokolle.
7. Fernzugriffsverbindungen zu lokalen und Cloud-Ressourcen sichern.
8. Ordnungsgemäße Verwaltung der Sicherheitswarnungen bei sämtlichen IIoT-Geräten und beim Cloud-System.
9. Ablaufpläne für Reaktionen auf bestimmte Vorfälle erstellen.
10. Bereitstellung von Plänen für Backups und Sicherheitstests.

### Granulare Anpassungsmöglichkeiten

Mit speziellen industriellen IoT-Plattformen (z.B. GE Predix oder Bosch IoT Suite) und Programmierschnittstellen (APIs=Application Programming Interfaces) lassen sich die spezifischen Ziele verschiedener Branchen leichter realisieren.

### Fragen zur Selbstkontrolle

1. Wie können IoT-Geräte mit einer einzigen Batterie über einen längeren Zeitraum, sogar bis zu zehn Jahre, betrieben werden, ohne dass die Batterie ausgetauscht werden muss?

*Low-Power-Wide-Area (LPWA)-Technologien wie Narrow-Band IoT (NB-IoT) und LoRaWAN ermöglichen den IoT-Geräten den Betrieb mit einer einzigen Batterie über einen längeren Zeitraum*

Zusammenfassung

Im Internet der Dinge (IoT) wird so gut wie jedes „Ding“ mit dem Internet verbunden, was erhebliche Auswirkungen auf unser tägliches Leben haben wird, von der Gesundheitsfürsorge bis zur Arbeitswelt. Die Implementierung und der Einsatz von IoT-Lösungen sind jedoch mit vielen Hindernissen und Herausforderungen verbunden, z. B. in Bezug auf Sicherheit, Datenschutz und Skalierbarkeit. Eine sorgfältige Planung sowie eine Architektur, die bestimmte Standards und Sicherheitsrichtlinien einhält, können den Systemverantwortlichen von IoT-Lösungen die Verwaltung, Fehlerbehebung, Skalierung und Anpassung der IoT-Netze erleichtern.

Verschiedene IoT-Einsatzfälle haben unterschiedliche Anforderungen an die Planung und Architektur. Das nicht-industrielle oder Verbraucher-IoT, zu dem z. B. Wearables und Smart Homes gehören, bietet Verbraucher:innen Komfort, indem es ihre täglichen Aufgaben automatisiert, ist in der Regel kostengünstiger und weist im Vergleich zu den industriellen IoT-Anwendungen ein geringeres Maß an Robustheit, Sicherheit, Skalierbarkeit und Langlebigkeit des Netzes auf. Beim IIoT, bei dem die industriellen Abläufe in verschiedenen Industriesektoren optimiert und die Effizienz mithilfe von Big Data und maschinellen Lernverfahren verbessert wird, müssen zusätzliche Anforderungen bei der Gestaltung der IIoT-Netzwerke berücksichtigt werden. Dazu gehört beispielsweise, dass industrielle IoT-Geräte und -Netzwerke extremen Umgebungsbedingungen wie hohen Temperaturen und Feuchtigkeit standhalten müssen. Außerdem sollten die Geräte in der Lage sein, ihre Daten über eine große Reichweite an die industriellen Steuersysteme zu übertragen und einen so geringen Stromverbrauch haben, dass sie über einen längeren Zeitraum mit einer einzigen Batterie betrieben werden können. Darüber hinaus müssen IIoT-Geräte hohen Cybersicherheitsstandards genügen, um wertvolle Daten und Vermögenswerte zu schützen.

# Lektion 2 – Angriffe auf das Internet der Dinge

**Lernziele**

Nach dem Abschluss dieser Lektion werden Sie...

... die Sicherheitsunterschiede zwischen IT-Netzwerken und IoT-Netzwerken benennen können.

... die Unterschiede zwischen IoT-Schwachstellen, -Bedrohungen und -Risiken erklären können.

... die Top Ten IoT-Schwachstellen auflisten können.

... in der Lage sein, verschiedene Angriffe auf das IoT in jeder Schicht des grundlegenden IoT-Technologiestacks zu identifizieren und Gegenmaßnahmen zu nennen.

# 1. Angriffe auf das Internet der Dinge

## Einführung

Das Internet der Dinge wird Teil unseres Alltags, und sowohl Verbraucher:innen als auch Unternehmen machen sich Gedanken über seine Sicherheit. IoT-Hardware, -Infrastruktur und -Systeme sammeln, übertragen, speichern und analysieren sensible persönliche und geschäftliche Daten und sind daher wahrscheinlich irgendwann Angriffen ausgesetzt. Böswillige Angreifende versuchen, IoT-Sensoren/Aktoren aus der Ferne zu kompromittieren, indem sie eine Vielzahl von Techniken anwenden, vom Diebstahl der Zugangsdaten bis hin zur Ausnutzung von Schwachstellen. Sobald Angreifende ein intelligentes Gerät kontrollieren, können sie es dazu benutzen, Daten zu stehlen oder zu versuchen, den Rest des angeschlossenen Netzwerks zu schädigen. IoT-Systeme sind für den Schutz der Daten vor böswilligen Angriffen auf die Cybersicherheit verantwortlich. Jeder Verlust, jede Beschädigung oder Zerstörung von IoT-Daten und Vermögenswerten kann verheerende Auswirkungen auf Einzelpersonen und Unternehmen haben.

Obwohl standardisierte Sicherheitstechniken für Informationstechnologie (IT-Systeme) vorhanden sind, könnte es eine Herausforderung sein, angemessene Sicherheitsmaßnahmen für IoT-Netzwerke zu implementieren. Gründe dafür sind die Komplexität von IoT-Geräten und -Netzwerken, das Fehlen von Anforderungen und Standard-Checklisten und die Exposition von IoT-Sensoren gegenüber der realen Welt. Da sich viele Hersteller von IoT-Sensoren auf Funktionen, Benutzerfreundlichkeit und niedrige Kosten bei ihren Produkte konzentrieren, haben IoT-Sensoren keine starke Sicherheitsausstattung. Dies sind einige der Gründe, warum IoT-Systeme im Vergleich zu IT-Netzwerken anfälliger für Cyberangriffe sind. In der folgenden Abbildung wird die Sicherheit von IoT-Netzen mit der von herkömmlichen IT-Netzen verglichen.

Traditionelle IT- versus IoT-Sicherheit

Quelle: Reza Vahidnia (2022) basierend auf Sulaiman (2019)

## Schwachstellen, Bedrohungen und Risiken

Um die IoT-Angriffe auf die Cybersicherheit besser zu verstehen und einen Plan für das Cyber-Risikomanagement entwickeln zu können, muss zunächst zwischen IoT-Schwachstellen, -Bedrohungen und -Risiken unterschieden werden. Diese drei gebräuchlichen Begriffe werden in der Regel synonym verwendet, unterscheiden sich jedoch grundlegend voneinander.

Eine Schwachstelle ist jede Unzulänglichkeit in IoT-Geräten, -Netzwerken, -Infrastrukturen oder -Anwendungen, die das gesamte IoT-System für Cyberangriffe anfällig machen kann. Eine Schwachstelle ist im Grunde eine Lücke im IoT-System, durch die böswillige Angreifende Zugang zu den IoT-Daten und -Anlagen erhalten können. Zwar sind Unternehmen aller Größenordnungen von Cyberangriffen betroffen, doch sind kleine und mittlere Unternehmen in der Regel stärker gefährdet, da nur wenige dieser Unternehmen eine Abteilung für Cybersicherheit einrichten können, die sich mit den Angriffen befasst.

Eine IoT-Bedrohung ist ein Prozess, der darauf abzielt, eine bestehende Schwachstelle auszunutzen und der die Wahrscheinlichkeit eines böswilligen Angriffs oder eines negativen Ereignisses vergrößert. Um festzustellen, wie man am besten mit Sicherheitsbedrohungen umgeht, sollten Unternehmen regelmäßig Bedrohungsanalysen und Penetrationstests (Erzeugung realer Bedrohungen) durchführen, um Schwachstellen zu entdecken.

Das Cybersicherheitsrisiko ist die Schnittmenge von Vermögenswerten und Daten, Bedrohungen und Schwachstellen (Glover, 2022). Cyberbedrohungen können potenziell zu Risiken für IoT-Daten und -Geräte führen und die Zerstörung oder Beschädigung von Daten oder Vermögenswerten verursachen (risk-vs-threat-vs-vulnerability, 2022). Mit anderen Worten: Die Kombination von Schwachstellen und Bedrohungen führt zu Risiken. Die folgende Abbildung fasst den Unterschied zwischen Schwachstelle, Bedrohung und Risiko zusammen.

Schwachstelle versus Bedrohung versus Risiko

Quelle: Reza Vahidnia (2022)

Lösungen für das Schwachstellenmanagement helfen Unternehmen und Organisationen, ihre Cybersicherheitsrisiken zu beherrschen, indem sie das Risiko niedrig und überschaubar halten. Traditionell würden Schwachstellenmanagementsysteme fast alles als Risiko betrachten. Sicherheitsteams müssten dann die Risiken nach Prioritäten ordnen und Abhilfe für die Risiken mit hoher Priorität schaffen. Dieser Ansatz würde zu einer Verschwendung von Ressourcen und Zeit führen, ohne für umfassende Sicherheit zu sorgen. Bei modernen oder risikobasierten Schwachstellenmanagementsystemen hingegen legen Unternehmen das für sie akzeptable Risikoniveau fest und nutzen dann Echtzeit-Bedrohungsdaten, Algorithmen für maschinelles Lernen und Datenwissenschaft, um ihre Hauptrisiken zu isolieren, zu priorisieren und zu verringern.

Die wichtigsten IoT-Schwachstellen

Quelle: Reza Vahidnia (2022), basierend auf Sheward (2020)

### Schwachstellen

**Hartkodierte Passwörter**

Im Quelltext eingebettete Zugangsdaten im Klartext.

Um das Problembewusstsein zu schärfen und zur Schaffung einer sichereren Welt beizutragen, hat eine freiwillige Gemeinschaft von Sicherheitsexpert:innen, das [Open Web Application Security Project](https://owasp.org/) (OWASP), die [Top Ten IoT-Schwachstellen identifiziert, die in der Abbildung oben dargestellt sind **Ungültige Quelle angegeben**.](https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf)

1. **Schwache Passwörter:** Die Verwendung leicht mit Brute Force zu knackenden, zu erratenden oder **hartkodierter** **Passwörter** gestattet unbefugten Zugriff auf die eingesetzten Systeme. Die Aktivierung einer Zwei-Faktor-Authentifizierung bietet eine zweite Sicherheitsebene für IoT-Geräte und -Systeme. Darüber hinaus bietet ein Kennwortverwaltungssystem die Möglichkeit, automatisch eindeutige Kennwörter für jeden Dienst zu generieren und die Benutzenden daran zu erinnern, ihre Kennwörter regelmäßig zu ändern.
2. **Unsichere Netzwerkdienste:** Unnötige offene Ports sind häufige Sicherheitsmängel, welche die Vertraulichkeit, Integrität, Authentizität oder Verfügbarkeit der Daten beeinträchtigen und eine unbefugte Fernsteuerung der IoT-Geräte ermöglichen können. Die Anzahl der offenen Ports sollte so gering wie möglich gehalten werden, um die Angriffsmöglichkeiten zu verringern.

#### Unsichere Ökosystem-Schnittstellen: Bei einer sicheren IoT-Lösung sollten alle Komponenten der Wertschöpfungskette, einschließlich Hardware, Konnektivität, Plattform und Anwendungen, gesichert sein. Die Anwendungsprogrammierschnittstellen (APIs) sowie die Mobil- und Webanwendungen, die den Nutzenden die Möglichkeit zur Interaktion mit den IoT-Geräten bieten, müssen sicher sein.

**Anwendungsprogrammierschnittstelle (API)**

Jede Software-Schnittstelle, die es Computern ermöglicht, miteinander zu kommunizieren.

#### Fehlen eines sicheren Update-Mechanismus: Mithilfe von Over-the-Air-Firmware-Updates (OTA-Updates) können Unternehmen die Sicherheitsfunktionen ihrer angeschlossenen Geräte aus der Ferne aktualisieren. Diese Firmware-Updates müssen sicher und zuverlässig über verschlüsselte Kanäle durchgeführt werden. Andernfalls kann es sein, dass das Gerät nicht mehr reagiert, wenn eine Aktualisierung nicht vollständig abgeschlossen wird.

#### Verwendung von unsicheren oder veralteten Komponenten: Die Verwendung unsicherer oder veralteter Softwarebibliotheken (z. B. Software von Drittanbietern oder Hardwarekomponenten aus einer kompromittierten Lieferkette) kann dazu führen, dass das Gerät gefährdet wird.

1. **Unzureichender Datenschutz:** Die wertvollen persönlichen oder geschäftlichen Daten der Nutzenden, die von den IoT-Geräten erfasst und auf ihnen gespeichert werden, können unsicher, unsachgemäß oder ohne Genehmigung verwendet werden.
2. **Unsichere Datenübertragung und -speicherung:** Die IoT-Daten im Speicher, bei der Übertragung oder bei der Verarbeitung in der Cloud müssen geschützt und verschlüsselt werden, um sicherzustellen, dass Unbefugte (Personen oder Anwendungen) keinen Zugriff auf sensible Daten haben.
3. **Fehlende Geräteverwaltung:** Das Gerätemanagement gibt einen vollständigen Überblick über den Status aller mit dem Netzwerk verbundenen IoT-Geräte an einem Ort. Ohne Gerätemanagement ist es nicht möglich zu wissen, ob ein IoT-Gerät angeschlossen und autorisiert ist, ob seine Firmware aktualisiert ist oder ob es die Daten ordnungsgemäß und sicher sendet.
4. **Unsichere Standardeinstellungen:** Einige IoT-Geräte werden möglicherweise mit unsicheren Standardeinstellungen ausgeliefert, damit die Betreiber ihre Tests und Konfigurationen durchführen können. Außerdem können einige Geräte nicht sicherer werden, weil die Benutzenden die Konfigurationen nur eingeschränkt ändern können.
5. **Fehlende physische Robustheit:** Ohne physische Sicherungsmaßnahmen, wie z. B. Manipulationssicherheit, können potenzielle Angreifende die lokale Kontrolle über die Geräte übernehmen oder sensible Informationen für die künftige Fernsteuerung der IoT-Sensoren erlangen.

### Bedrohungen

Bei allen Bedrohungen der Cybersicherheit suchen Angreifende nach einer Schwachstelle im IoT-System, die sie ausnutzen können. Im Allgemeinen gibt es folgende drei Arten von IoT-Sicherheitsbedrohungen (Glover, 2022):

**Beabsichtigte Bedrohungen**

Absichtliche Bedrohungen sind Techniken und Aktivitäten, die von böswilligen Benutzenden und Angreifenden durchgeführt werden, um ein Sicherheits- oder IoT-System zu gefährden. Zu diesen Bedrohungen gehören:

* Malware ist jede Software, die gefährliche ausführbare Dateien in das System einschleust und Störungen der Hardware und des Netzwerks verursacht, private Daten weitergibt und unbefugten Zugriff auf das System ermöglicht.
* Ransomware ist eine Art von Malware, die das Opfer zur Zahlung eines Lösegelds auffordert. Andernfalls werden die privaten Daten des Opfers veröffentlicht oder der Zugriff auf die Daten dauerhaft gesperrt.
* Phishing ist das Versenden einer betrügerischen Nachricht durch die Angreifenden, die eine Person dazu zu verleiten soll, ihre sensiblen Daten wie Anmeldeinformationen preiszugeben oder Ransomware auf dem Zielsystem zu installieren.

**Unbeabsichtigte Bedrohungen**

Unbeabsichtigte Bedrohungen sind in der Regel auf menschliches Versagen zurückzuführen, z. B. wenn jemand sensible Daten ungeschützt lässt oder vergisst, die Firewall-Software zu aktualisieren.

**Natürliche Bedrohungen**

Naturereignisse wie Wirbelstürme, Überschwemmungen und Erdbeben können die IoT-Infrastruktur beschädigen (insbesondere die Sensoren, die der realen Welt ausgesetzt sind).

### Risiken

Da Unternehmen und Organisationen in fast allen Branchen immer mehr auf IoT-Geräte setzen, sollten IoT-Sicherheitsteams sowohl einfache als auch komplexe IoT-Risikofaktoren berücksichtigen. Die folgenden sechs IoT-Risiken sollten beachtet werden:

#### Botnetze

Da intelligente IoT-Objekte in der Regel nicht über die gleichen fortschrittlichen eingebauten Sicherheitsmechanismen verfügen wie Computer, die an ein herkömmliches IT-Netz angeschlossen sind, sind sie anfälliger für Malware. Angreifende bilden Botnetze, indem sie mehrere IoT-Geräte mit Malware infizieren. Diese Armee infizierter Geräte kann dann die anderen Systeme innerhalb des Netzwerks angreifen und sie mit Datenverkehr oder Spam-Daten überfluten.

#### Ransomware

Anstelle von kritischen Daten können Angreifende auch kritische IoT-Geräte ins Visier nehmen (z. B. das Anhalten einer Sicherheitskamera oder eines wichtigen Industriesensors), um den grundlegenden Betrieb eines Unternehmens oder einer Organisation zu stören.

#### Konvergenz

Die traditionellen IT-Netzwerke, die IoT-Geräte und die Betriebstechnologie sind heutzutage alle mit dem Internet verbunden, was alle drei Systeme anfälliger für IoT-Cyberangriffe macht.

#### Unsichtbarkeit

Jede Sicherheitsbedrohung für die IoT-Geräte kann durch die Sichtbarkeit der Geräte und die Überwachung des Datenverkehrs, der durch sie fließt, identifiziert werden. IoT-Sicherheitsteams werden nicht in der Lage sein, unsichtbare IoT-Geräte zu schützen.

#### Nichtverschlüsselte Daten

**Hijacking**

Übernahme der Kontrolle über IoT-Systeme, Programme oder Kommunikationswege.

Die meisten preiswerten IoT-Geräte verfügen nicht über eingebaute Ressourcen für eine starke Datenverschlüsselung bei der Übertragung sensibler Daten in die Cloud. Somit wird die Übertragung anfällig für Abhören (Angreifende hören mit und zeichnen die Daten auf, die zwischen dem IoT-Gerät und der Cloud ausgetauscht werden), Spionage (Zugriff auf sensible Daten zur Erzielung wirtschaftlicher Gewinne) und **Hijacking**. Auf diese Weise können Angreifende beispielsweise die Aufzeichnung eines Sicherheitsmikrofons stoppen oder wichtige Daten eines angeschlossenen Fahrzeugs verändern.

#### Rogue-Geräte

Rogue-Geräte sind Ersatz für legitime Sensoren, die Angreifenden Rogue-Zugangspunkte bieten und es ihnen ermöglichen, das Netzwerk zu kontrollieren und die Daten zu ändern oder zu stehlen.

### Fragen zur Selbstkontrolle

1. Bitte erläutern Sie, warum unsichere Netzwerkdienste als Schwachstelle für IoT-Systeme gelten.

Unnötige offene Ports sind häufige Sicherheitsmängel, welche die Vertraulichkeit, Integrität, Authentizität oder Verfügbarkeit der Daten beeinträchtigen und eine unbefugte Fernsteuerung der IoT-Geräte ermöglichen können.

## 2.2 Cyberangriffe und Gegenmaßnahmen

Ein erster Schritt zur Bewältigung der IoT-Cyberbedrohungen besteht darin, diese auf jeder Ebene der IoT-Architektur zu verstehen. Das Open Web Application Security Project (OWASP), ein Komitee von freiwilligen Sicherheitsexpert:innen, hat eine detaillierte Liste entworfen und veröffentlicht, in der aufgeführt wird, in welchen Bereichen von IoT-Lösungen Schwachstellen oder Bedrohungen vorhanden sein können. Diese Veröffentlichung zeigt, dass alle wesentlichen Komponenten einer IoT-Lösung von Angreifenden ausgenutzt werden können. Die von OWASP identifizierte IoT-Angriffsfläche umfasst (Chang & Li, 2019)

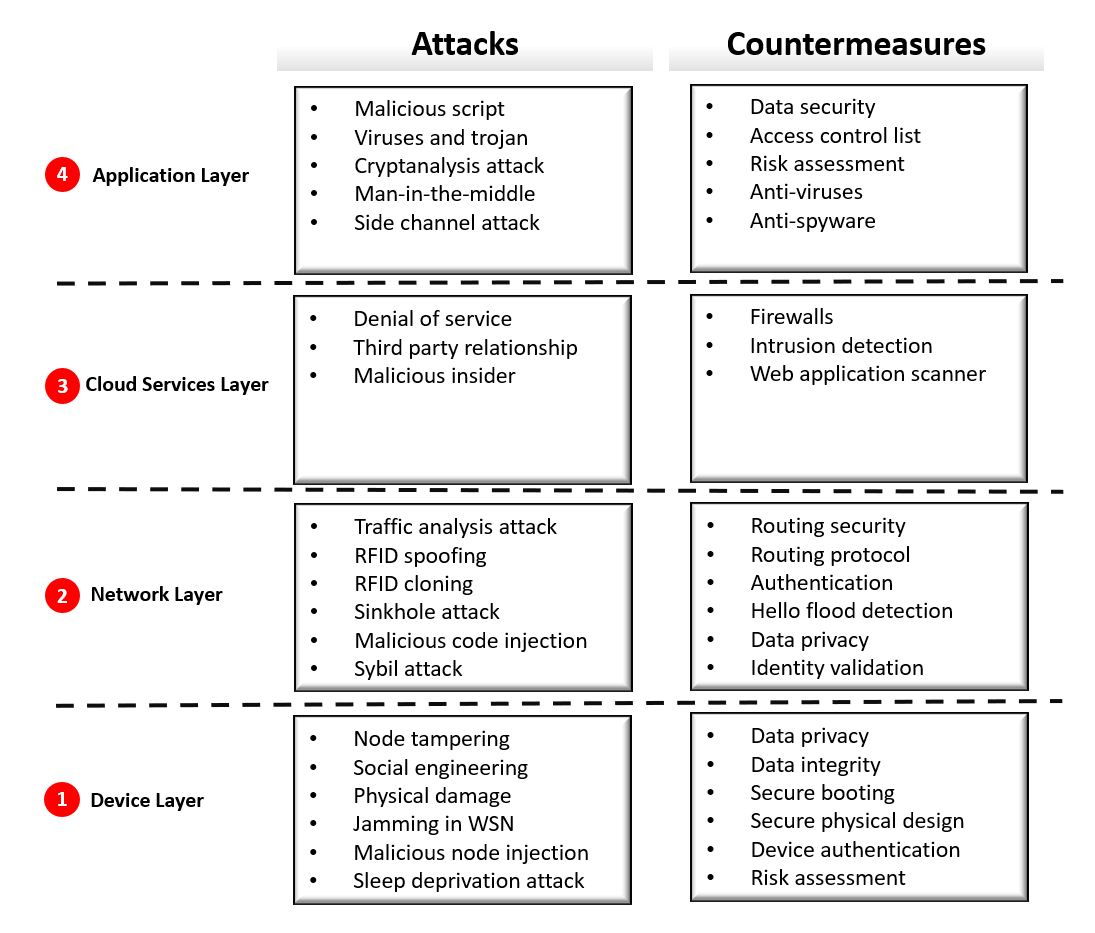
* **Geräte.** Die Schwachstellen können am Speicher des Geräts, an der physischen Schnittstelle, an der Firmware, am Web-Interface und an den Netzwerkdiensten vorliegen. Darüber hinaus sind die ungesicherten Standardeinstellungen des Geräts, veraltete Komponenten und ungesicherte Aktualisierungsmechanismen einige Schwachstellen, die Angreifende ausnutzen können. Die Hersteller von IoT-Geräten müssen sicherstellen, dass die intelligenten Objekte nur mit den zugelassenen Diensten und der zugelassenen Hardware in Kontakt kommen und dass ihre Anweisungen nicht durch schädliche Programmcodes ersetzt werden, die den Betrieb des Geräts beeinträchtigen.
* **Konnektivität.**Cyberbedrohungen können von den Kommunikationskanälen ausgehen, die verschiedene IoT-Komponenten miteinander verbinden. Das gesamte IoT-Netz kann von Sicherheitsproblemen bei den Kommunikationsprotokollen sowie von Netzangriffen wie Spoofing (Tarnung einer Kommunikation von einer unbekannten Quelle als von einer vertrauenswürdigen Quelle stammend) und Denial-of-Service (Unterbrechung der Dienste eines Servers) betroffen sein.
* **Anwendungen und Software.** Angreifende können die IoT-Systeme kompromittieren, indem sie die Schwachstellen der Webanwendungen und der Software ausnutzen, um Anmeldedaten zu stehlen oder bösartige Firmware-Updates zu versenden.

Um die Sicherheit besser in alle Schichten und Aspekte einer IoT-Lösung vom Gerät bis zur Gesamtkonfiguration zu integrieren, muss sie bereits in der ersten Entwurfsphase berücksichtigt werden. Einige Sicherheitsrichtlinien, die bei der Konzeption und Entwicklung einer IoT-Lösung zu berücksichtigen sind, lauten wie folgt (Chang & Li, 2019):

* Alle gesammelten und gespeicherten Daten wie Sensordaten und Zugangsdaten sollten entsprechend zugeordnet und erfasst werden.
* Bei der Konfiguration von IoT-Geräten sollte auf die Sicherheit geachtet werden. Mit anderen Worten: Bevor ein intelligenter Sensor an das Netz angeschlossen wird, sollten die Einstellungen gesichert werden. Zu den Maßnahmen zur Sicherung der Einstellungen gehören Verschlüsselung, mehrstufige Authentifizierung sowie ein sicherer Benutzername und ein sicheres Passwort.
* Um die Auswirkungen von Cyberangriffen zu verringern und die Risiken zu mindern, sollten Unternehmen ihre Sicherheitsstrategie in der Annahme entwickeln, dass es keine perfekte Verteidigung gegen sich entwickelnde Sicherheitsbedrohungen gibt.
* Die zugänglichen IoT-Geräte sollten physisch gesichert und gegen Manipulationen geschützt sein.

Die folgende Abbildung fasst die Sicherheitsangriffe und die entsprechenden Gegenmaßnahmen auf jeder Schicht des grundlegenden IoT-Technologiestacks zusammen (Najmi et al., 2021).

IoT-Angriffe und Gegenmaßnahmen



Quelle: Reza Vahidnia (2022), basierend auf Najmi et al. (2021)

Im Folgenden werden die Angriffe und Gegenmaßnahmen für jede Schicht des grundlegenden IoT-Technologiestacks näher erläutert (Deogirikar & Vidhate, 2017).

### Geräte-Schicht

Die physischen Angriffe auf der Hardware-Ebene zielen auf IoT-Geräte ab. Zu diesen Angriffen gehören Knotenmanipulation, physische Beschädigung von Knoten, Social Engineering, Jamming, Einschleusung bösartiger Knoten und Schlafentzug.

#### Knotenmanipulation

Angreifende können den kompromittierten Knoten physisch verändern und sensible Daten wie Verschlüsselungscodes erlangen. Die Implementierung von Authentifizierungsalgorithmen zur Erkennung manipulierter Geräte ist nützlich, um solche Angriffe abzuwehren.

#### Social Engineering

Bei Social-Engineering-Angriffen handelt es sich um psychologische Angriffe auf Menschen, die Geräte benutzen, und nicht auf die Geräte selbst. Angreifende kommunizieren mit dem Opfer, um die Preisgabe sensibler Informationen (z. B. einer Kreditkartennummer) zu veranlassen oder um zu erreichen, dass die Person eine kritische Aktion durchführt (z. B. eine bestimmte Website aufruft). Die verfügbaren Gegenmaßnahmen zum Schutz von IoT-Systemen gegen Social-Engineering-Angriffe werden in trainingsbasierte und automatische Abwehrmaßnahmen unterteilt. Bei der trainingsbasierten Abwehr werden die Benutzenden so geschult, dass sie sich auf der Grundlage der aus früheren Angriffen gewonnenen Erkenntnisse selbst schützen können. Bei automatischen Verfahren werden Phishing-Versuche automatisch erkannt, indem die Kommunikation analysiert und Merkmale wie irreführende URLs (Uniform Resource Locators), Passwortanfragen und das Vorhandensein bestimmter Bilder identifiziert werden (Harris, 2022).

#### Physische Beschädigung

Angreifende können die IoT-Geräte oder andere Komponenten des IoT-Systems physisch beschädigen, um einen Denial-of-Service zu verursachen. Die physische Sicherung der IoT-Geräte und deren Schutz vor Manipulation ist eine Lösung zur Abwehr solcher Angriffe.

#### Jamming

Das Ziel von Jamming-Angriffen in drahtlosen Sensornetzwerken (WSNs) besteht darin, die drahtlose Kommunikation zwischen den Knoten des Netzwerks zu stören. Die zwei Hauptarten von Jamming-Angriffen sind proaktiv und verschleiert. Beim proaktiven Jamming, welches die am weitesten verbreitete Form ist, werden unabhängig vom Muster des Datenflusses im Kommunikationskanal Störsignale ausgesendet. Aufgrund dieses Mangels an Anpassung an den Kommunikationskanal ist diese Störattacke ineffizient. Beim verschleierten Jamming werden statt zufälliger Bits reguläre, legitime Datenpakete übertragen, was die Entdeckung des Angriffs erschwert. Zur Bekämpfung von Jamming-Angriffen werden verschiedene Methoden eingesetzt, darunter Spreizspektrum-Techniken wie Direct Sequence Spread Spectrum (DSSS) und Frequenzsprung-Spreizspektrum (FHSS; Hymlin Rose & Jayasree, 2019).

#### Einschleusung bösartiger Knoten

Bei dieser Art des Angriffs wird ein bösartiger Knoten zwischen zwei weiteren Knoten platziert, um die Daten zu verändern, welche die Knoten passieren. Eine Möglichkeit, diesen Angriff zu verhindern, ist die Verwendung eines Monitoring Verification-Schemas (MOVE-Schema), das die Knoten überprüfen und jegliches böswillige Verhalten erkennen kann.

#### Schlafenzugs-Angriff

Das Ziel dieses Angriffs ist es, den Stromverbrauch der IoT-Knoten so zu erhöhen, dass sie abgeschaltet werden müssen. Dies wird erreicht, indem der angreifende Knoten den Zielknoten daran hindert in den Ruhezustand zu gehen. Defensivalgorithmen, die den lokalen Batterieverbrauch der IoT-Geräte überwachen, können verwendet werden, um das Risiko von Schlafentzugsangriffen zu mindern.

### Netzwerkschicht

Die folgenden Angriffe konzentrieren sich auf das IoT-Netzwerk und die Kommunikationskanäle.

#### Verkehrsanalyse-Angriffe

Angreifende fangen die IoT-Nachrichten ab und belauschen sie, um Zugriff auf Netzwerkinformationen zu erhalten. Eine gängige Methode zur Abwehr solcher Angriffe besteht darin, den Datenverkehr undurchsichtig zu machen, indem Pakete aufgefüllt, mit einer konstanten Rate übertragen und Dummy-Pakete eingeschleust werden.

#### RFID-Spoofing

Unter Kenntnis der Kommunikationsprotokolle und Authentifizierungen geben Angreifende einen gültigen RFID-Tag vor, um dessen Rechte zu erlangen. Dazu verwenden sie spezielle Geräte mit erweiterter Funktionalität, die in der Lage sind, den RFID-Tag nachzuahmen und die von den Tags übertragenen RFID-Signale zu fälschen. In anderen Worten ausgedrückt, bei diesen Angriffen werden dem IoT-System falsche Informationen übermittelt, die scheinbar richtig sind.

#### RFID-Klonen

Bei einem Klon-Angriff kopieren Angreifende die Informationen von einem bereits vorhandenen RFID-Tag auf einen anderen RFID-Tag und fügen dann falsche Informationen ein oder kontrollieren die Daten, die durch den geklonten Tag laufen. Eine Möglichkeit zur Vermeidung von RFID-Klonen besteht darin, einen RFID-Tag zu verwenden, der eine Verschlüsselungstechnologie unterstützt (bei RFID-Tags und -Lesegeräten, die gemäß der Norm ISO 14443 hergestellt werden, ist dies der Fall). Bei diesen gesicherten Tags autorisiert das RFID-Lesegerät nur RFID-Tags mit dem richtigen Schlüssel.

#### Sinkhole-Angriff

Bei diesem aktiven Angriff führen Angreifende ihre Attacke über einen kompromittierten Knoten im Netz aus. Um den IoT-Verkehr anzulocken und dann die Daten zu verändern, sendet der kompromittierte Knoten falsche Routing-Informationen an seine Nachbarn und teilt ihnen mit, dass er die geringste Entfernung zur Basisstation hat. Eine Möglichkeit, Sinkhole-Angriffe zu erkennen und den gefährdeten Knoten zu identifizieren, besteht darin, den minimalen Hop Count des Knotens mit dem berechneten durchschnittlichen Hop Count des Netzwerks zu vergleichen. Wenn der minimale Hop Count erheblich kleiner ist als der Durchschnittswert, dann könnte im Netz ein Sinkhole-Angriff vorliegen.

#### Einschleusung von bösartigem Code

Bei diesem Angriff, der von OWASP als eine der gravierendsten API-Sicherheitsschwachstellen eingestuft wird, injizieren Angreifende über ein Benutzereingabefeld physisch Schadcode in eine Software oder Anwendung, um die vollständige Kontrolle über das IoT-Netzwerk zu erlangen. Zu den grundlegenden Praktiken zur Vermeidung dieser Art von Angriffen gehören die Validierung von Benutzereingaben mit Erlaubnislisten und die Codierung von HTML-Ausgaben, um bösartige Eingaben in sichere Formate zu übersetzen.

#### Sybil-Attacke

Bei diesem Angriff betreibt ein einzelner Knoten in einem Peer-to-Peer-Netz viele aktive gefälschte Identitäten gleichzeitig, um die Autorität oder Macht in einem seriösen System (z. B. einem Wahlsystem) zu untergraben, indem er den größten Einfluss im Netz erlangt. Zu den Maßnahmen zur Verhinderung von Sybil-Angriffen gehören Identitäts- und Persönlichkeitsüberprüfung, Graphalgorithmen für soziale Vertrauenswürdigkeit und anwendungsspezifische Techniken.

### Schicht der Cloud-Dienste

#### Denial-of-Service (DoS)

Bei dieser Art von Angriff überfluten Angreifende das Netzwerk mit überwältigendem Datenverkehr, so dass die Cloud-Dienste und -Ressourcen für die vorgesehenen Nutzenden nicht mehr verfügbar sind. Intrusionserkennungssysteme und Firewalls, die als verkehrsüberwachende Barrieren zwischen den Netzknoten fungieren, können eingesetzt werden, um das Risiko von DoS-Angriffen zu mindern.

#### Drittanbieter-Beziehung

Ein Angriff über eine Drittanbieter-Beziehung wird auch als Lieferkettenangriff (Supply Chain Attack) bezeichnet. Er findet statt, wenn eine Person das IoT-System über einen Partner oder Anbieter infiltriert, der Zugang zum IoT-System und zu den Daten hat.

#### Böswilliger Insider

Ein böswilliger Insider ist eine Person, die Kenntnis von geschützten Daten eines Unternehmens erlangt hat und diese absichtlich missbraucht, um die Integrität des Unternehmens zu beeinträchtigen. Dieser Sicherheitsangriff kann durch die Überwachung der Benutzeraktivitäten, die Untersuchung der Vorfälle und die Zugangsverwaltung aufgedeckt werden.

### Anwendungsschicht

#### Bösartiges Skript

Bei Angriffen mit bösartigen Skripten oder Cross-Site-Scripting (XSS) können Angreifende durch Einschleusen bösartiger Skripte Zugriff auf die Anwendung erlangen. Um diese Art von Angriffen zu verhindern, sollte die Anwendung alle Eingabedaten validieren, um sicherzustellen, dass nur Daten eingegeben werden, die auf einer Erlaubnisliste stehen und dass alle variablen Ausgaben einer Seite verschlüsselt werden, bevor sie an Benutzende zurückgegeben werden.

#### Viren und Würmer

Ein Angreifender kann das IoT-System durch bösartige Programmcodes wie Viren und Würmer beschädigen (Computerwürmer replizieren sich ohne menschliches Zutun). Diese bösartigen Codes können durch E-Mail-Anhänge oder durch das Herunterladen von Dateien aus dem Internet verbreitet werden. Virenscanner, Firewalls und Systeme zur Erkennung von Eindringlingen sind einige Werkzeuge, die diese bösartigen Codes aufspüren und entfernen.

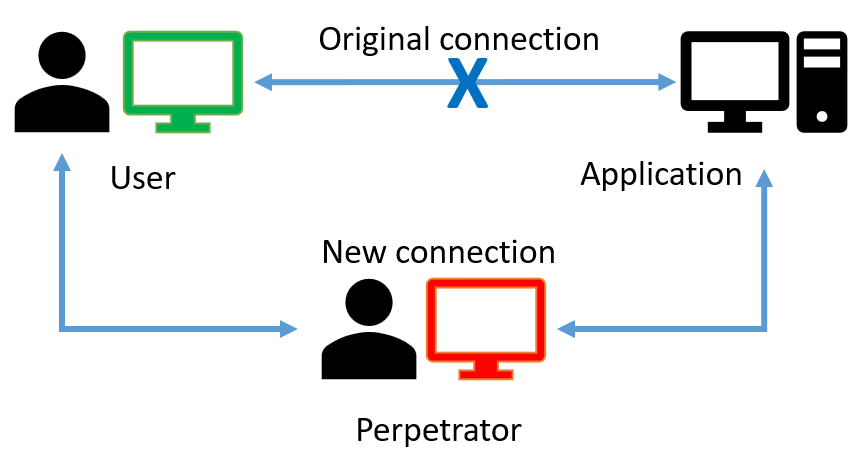
#### Kryptoanalyse-Angriff

Bei dieser Art von Angriff verwenden Angreifende Klartext oder Chiffretext, um Kodierungsschlüssel zu erhalten. Um das IoT-System vor Kryptoanalyse-Angriffen zu schützen, sollten die Daten angemessen verschlüsselt werden, so dass sie selbst dann unlesbar sind, wenn sie böswilligen Angreifenden in die Hände geraten. Darüber hinaus sollten für die Verschlüsselung starke und eindeutige Schlüssel verwendet und an einem sicheren Ort aufbewahrt werden.

#### Man-in-the-Middle (MITM)

Bei dieser Art von Cyberangriff fangen Angreifende die Kommunikation zwischen zwei Knoten ab, um durch Abhören an sensible Daten zu gelangen. Die Verwendung virtueller privater Netzwerke (VPN) und die Verschlüsselung der Datenkommunikation sind bewährte Verfahren zur Verhinderung eines Man-in-the-Middle-Angriffs.

Man-in-the-Middle-Angriff



Quelle: Reza Vahidnia (2023)

#### Seitenkanal-Angriff

Bei diesem passiven Sicherheitsangriff, der in der Regel schwer zu erkennen ist, nutzen Angreifende die Informationen des Seitenkanals (z. B. Informationen über die Leistung, die für die Durchführung des Vorgangs benötigte Zeit, die Fehlerfrequenz), die von den verschlüsselnden Geräten ausgesendet werden, um den Verschlüsselungscode zu ermitteln.

### Fragen zur Selbstkontrolle

1. Bitte erklären Sie die Funktionsweise und die Absicht eines Denial-of-Service-Angriffs. Nennen Sie auch eine Gegenmaßnahme zur Verhinderung eines DoS-Angriffs.

Bei dieser Art von Angriff überfluteten Angreifende das Netzwerk mit überwältigendem Datenverkehr, so dass die Cloud-Dienste und -Ressourcen für die vorgesehenen Nutzenden nicht mehr verfügbar sind. Intrusionserkennungssysteme und Firewalls, die als verkehrsüberwachende Barrieren zwischen den Netzknoten fungieren, können eingesetzt werden, um das Risiko von DoS-Angriffen zu mindern.

1. Bitte erklären Sie den Zweck eines Sinkhole-Angriffs.

Ziel dieses Angriffs ist es, den IoT-Datenverkehr über einen kompromittierten Knoten anzulocken und dann die Daten zu verändern.

1. Bitte wählen Sie aus, bei welcher Angriffsart ein Angreifender den Klartext oder den Chiffretext verwendet, um die Verschlüsselungscodes zu erhalten.

* Böswilliger Insider
* Seitenkanal-Angriff
* *Kryptoanalyse-Angriff*
* Man-in-the-Middle-Angriff

1. Bitte nennen Sie sechs IoT-Angriffe auf der Geräteebene des grundlegenden IoT-Technologiestacks.

Knotenmanipulation

Social Engineering

Physische Beschädigung

Jamming in WSN

Einschleusung bösartiger Knoten

Schlafenzugs-Angriff

Zusammenfassung

Im Vergleich zu herkömmlichen IT-Netzen sind die Sicherheitsaspekte von IoT-Systemen vielschichtiger. Die Umsetzung von Sicherheitsmaßnahmen in IoT-Systemen stellt aufgrund der Komplexität von IoT-Geräten und -Netzen, des Fehlens von Anforderungen und Standard-Checklisten und der Exposition von IoT-Sensoren gegenüber der realen Welt eine größere Herausforderung dar.

Um ein IoT-System vor Cyberangriffen zu schützen, müssen zunächst die Schwachstellen, Bedrohungen und Risiken, die auf jeder Ebene des grundlegenden IoT-Technologiestacks auftreten können, ermittelt und verstanden werden.

Zu den Cyberangriffen in der Schicht der Dinge gehören Knotenmanipulation, physische Beschädigung von Knoten, Social Engineering, Jamming, Einschleusung bösartiger Knoten und Schlafentzug, die auf die IoT-Geräte abzielen. In der Kommunikationsschicht (Konnektivität) liegt der Fokus der Angreifenden auf dem IoT-Netzwerk und den Kommunikationskanälen. Sie versuchen, die zwischen den IoT-Knoten und der Cloud ausgetauschten Daten zu manipulieren, den Datenverkehr zu analysieren oder bösartigen Code einzuschleusen, um die Kontrolle über das Netzwerk zu erlangen. Denial-of-Service-Angriffe, Drittanbieter-Angriffe und böswillige Insider sind einige IoT-Angriffe, die sich auf das Software-Backend und Cloud-Dienste beziehen. In der Anwendungsschicht konzentrieren sich die Angriffe hauptsächlich auf den Zugriff auf die Anwendungsdaten, z. B. auf die Verschlüsselungscodes.

Für alle oben genannten vier Schichten des grundlegenden IoT-Technologiestacks haben wir die Maßnahmen erörtert, mit denen Cyberangriffen entgegengewirkt werden kann.

# Lektion 3 – Security by Design

**Lernziele**

Nach dem Abschluss dieser Lektion werden Sie...

... die sieben Phasen im Lebenszyklus der Softwareentwicklung auflisten und erläutern können.

... in der Lage sein, die Vorteile der Umsetzung eines sicheren Produktlebenszyklus in der Softwareentwicklung zu beschreiben.

... die Unterschiede zwischen statischem und dynamischem Testen erklären können.

... fähig sein, die Vor- und Nachteile von statischen und dynamischen Tests zu benennen.

... das Konzept von DevSecOps und dessen Unterschied zu DevOps erläutern können.

# 3. Security by Design

## Einführung

Bei vielen IoT-Projekten in der Vergangenheit, bei denen die Markteinführung oder andere Designüberlegungen für die Entwickelnden hohe Priorität hatten, wurde die Sicherheit erst in fortgeschrittenen Phasen (z. B. beim Prototyping) der Produktentwicklung als zusätzliches Element in Betracht gezogen. Da IoT-Lösungen nicht einfach aufgerüstet werden können, war dieser Ansatz teuer und zeitaufwändig. So kann beispielsweise die Firmware von schwer zugänglichen und unsicheren Geräten nicht ohne weiteres auf einen neuen Stand gebracht werden, um Sicherheitsbedrohungen zu bekämpfen. Daher kann dieser Ansatz zu verheerenden Sicherheitslücken führen.

Im Rahmen des Konzepts „Security by Design“ wird die Vorplanung der Sicherheit bereits beim ersten Projektentwurf berücksichtigt und ist in allen Phasen der IoT-Produktentwicklung ein wichtiges Ziel, um Daten und Geräte zu schützen. Dabei wird eine Sicherheitsrisikoanalyse durchgeführt, um die Schwachstellen und die Auswirkungen der einzelnen Sicherheitsbedrohungen auf das IoT-System zu ermitteln. Dadurch können IoT-Architekt:innen geeignete Sicherheitsmaßnahmen finden und umsetzen, um den ermittelten Bedrohungen zu begegnen.

## 3.1 Projektmanagement und der sichere Entwicklungs-Lebenszyklus

Der Softwareentwicklungs-Lebenszyklus (Software Development Life Cycle, SDLC) ist ein standardisierter, schrittweiser Prozess, der von Entwickelnden verwendet wird, um qualitativ hochwertige Softwareprodukte zu erstellen und zu verifizieren. Er erlaubt einen besseren Überblick über das Projekt und ermöglicht die Risikominderung und Fehlerbeseitigung. Außerdem bietet er den Entwickelnden auch die Möglichkeit, den Fortschritt des Projekts zu verfolgen und sicherzustellen, dass alle Ziele und Anforderungen erreicht werden. Die Sicherheitsanforderungen des SDLC sind in der Norm ISA 62443-4-1 genau definiert. Diese Norm, die für die Entwicklung neuer und bestehender Software und Hardware gilt, definiert den Prozess, mit dem sichergestellt wird, dass die Sicherheit in den Produktentwurf integriert wird. Darüber hinaus behandelt sie verschiedene Testbereiche wie die statische Code-Analyse (SOA), die Analyse der Angriffsfläche und Blackbox-Tests für bekannte Schwachstellen (ISA 62443-4-1 Standards - SDLC Requirements, n.d.).

Softwareentwickelnde verwenden verschiedene [SDLC-Modelle](https://www.synopsys.com/blogs/software-security/top-4-software-development-methodologies/?intcmp=sig-blog-sdlc) wie z. B. Wasserfall- und Agile Methoden. Im Allgemeinen besteht der SDLC aus sieben Phasen, wie in der folgenden Abbildung dargestellt (Hammer, 2021).

Softwareentwicklungs-Lebenszyklus (SDLC)

Quelle: Reza Vahidnia (2022) basierend auf **Ungültige Quelle angegeben.**

### SDLC-Phasen

#### 1. Anforderungen und Analyse

Um die Probleme zu identifizieren, die von den Softwareentwickelnden angegangen werden sollten, wird ein Business Specification Document (BSD) erstellt, in dem die technischen, Markt- und Kundenanforderungen erfasst werden.

#### 2. Projektplanung

Auf der Grundlage des BSD wird das Softwareentwicklungsprojekt, unabhängig davon, ob es sich um ein neues Produkt oder ein Upgrade bestehender Software handelt, geplant (z. B. Risiken, Chancen, Probleme usw.) und in einer Software Requirements Specification (SRS, entspricht Lasten- und Pflichtenheft) festgehalten.

#### 3. Design

In Phase 3 werden von den Entwickelnden einzelne oder mehrere Konzepte vorgestellt, welche die primäre Ressource für den Aufbau des Projekts darstellen und in einer Design Document Specification (DDS) dokumentiert werden.

#### 4. Programmierung und Implementierung

Mit Hilfe von Programmiersprachen (z. B. C++, Python usw.) und Werkzeugen wie Compilern und Debuggern werden in dieser Phase die Programme geschrieben.

#### 5. Testen

In dieser Phase wird die Software auf Fehler getestet, um ihre Qualität zu gewährleisten. Die Tests können manuell oder automatisch mit Hilfe von Testwerkzeugen durchgeführt werden.

#### 6. Einsatz

Der nächste Schritt nach dem Testen ist die Auslieferung der Software an die Kundschaft, die sie einsetzt.

#### 7. Wartung

In dieser Phase werden die von der Kundschaft bemängelten Softwarefehler und Probleme behoben. Um den Wartungsaufwand zu reduzieren, wird die Software in der Regel zunächst nur für eine begrenzte Anzahl von Nutzenden freigegeben. Nach letzten Anpassungen wird die endgültige Version einer größeren Gruppe von Nutzenden angeboten.

### Sicherer SDLC

In den frühen SDLC-Systemen wurde die Sicherheit von vielen Softwareentwickelnden als Engpass für die Markteinführung neuer Produkte angesehen, da sie ihren endgültigen Programmcode überarbeiten und korrigieren mussten, um Sicherheitsprobleme zu vermeiden. Bei diesen Systemen begannen die sicherheitsrelevanten Aktivitäten im Grunde genommen in der Testphase des SDLC, und manchmal wurde aus Zeitgründen unsichere Software freigegeben. Ein solcher Ansatz kann ein Unternehmen gefährden, denn ein Sicherheitsrisiko für die Software bedeutet ein Risiko für den Betrieb, der die Software verwendet. Mit anderen Worten: Um das Unternehmen zu sichern, sollte die Software gesichert sein.

Kompromittierte Software, die zu Datenschutzverletzungen und Sicherheitsangriffen führt, kann verheerende Auswirkungen auf Unternehmen und Organisationen haben. Daher muss die Sicherung des SDLC für die Unternehmen eine hohe Priorität haben, und in jeder Phase des SDLC müssen Sicherheitsmaßnahmen getroffen werden. Wenn Sicherheitsprobleme in den frühen Phasen des SDLC nicht erkannt werden, ist ihre Behebung in den späteren Entwicklungsphasen teurer und zeitaufwändiger.

Die Sicherheitsschwachstellen eines Quelltextes können billiger und schneller aufgedeckt werden, wenn die Sicherheit in alle Phasen des bestehenden SDLC integriert wird. Die Verwendung dieses sicheren SDLC-Ansatzes, der die Systemarchitektur in der Entwurfsphase analysiert, die Programmierungen in der Erstellungsphase überprüft und vor der Freigabe der Software-Tests durchführt, verringert ebenfalls die Risiken des Unternehmens. Die folgenden Schritte sind für Organisationen und Unternehmen notwendig, um einen sicheren SDLC zu realisieren (Freeman, 2022):

* Einarbeitung der Entwickelnden in die besten sicheren Programmierverfahren und Frameworks.
* Analyse des Risikos der Systemarchitektur zu Beginn des Projekts.
* Berücksichtigung der Sicherheit der Tests in der Planungs- und Erstellungsphase.
* Schulung der Entwickelnden in der Verwendung von Programmcode-Test-Tools (z. B. SAST und DAST)
* Ausbildung der Entwickelnden zum Schreiben von sicherem Quelltext.

Unternehmen sollten auch [ein Software-Sicherheitsprogramm (SSP)](https://www.synopsys.com/blogs/software-security/bsimm-software-security-activities/l?intcmp=sig-blog-sdlc)  aufstellen, in dem sie erreichbare Ziele mit definierten Erfolgskennzahlen festlegen.

### Fragen zur Selbstkontrolle

1. Bitte wählen Sie aus, welche Phase des SDLC nach der Programmierungs- und Implementierungsphase durchgeführt wird.

* Testen
* Einsatz
* Wartung
* Sammeln der Anforderungen

## 3.2 Statisches Testen

Cyber-Angreifende suchen ständig nach neuen Wegen, um Software-Schwachstellen auszunutzen. Daher sollten Softwareentwickelnde ihre Anwendungen durch mehrere Testarten (z. B. funktionale Tests) schützen, sodass mit im Voraus erdachten Sicherheitsproblemen korrekt umgegangen wird. Durch Funktionstests werden jedoch nicht die Sicherheitslücken aufgedeckt, die zu Datenschutzverletzungen führen. Darüber hinaus verfügen IoT-Anwendungsentwickelnde möglicherweise nicht über einen soliden sicherheitstechnischen Hintergrund, um alle Sicherheitsaspekte im Voraus zu berücksichtigen und ihre Programmcodes ordnungsgemäß zu sichern oder Sicherheitsrisiken wie die Verwendung unsicherer APIs zu vermeiden.

Static Application Security Testing (SAST, statisches Software-Testverfahren) ist eine Scan-Methode oder ein Tool, das Entwickelnden dabei hilft, ihre Quell- oder Assembler-Codes zu überprüfen, bevor sie kompiliert werden, um Sicherheitsschwachstellen (z. B. die zehn größten von OWASP identifizierten Sicherheitsschwachstellen) in frühen Entwicklungsphasen zu entdecken. SAST wird auch als White- oder Open-Box-Testing bezeichnet, da der Quellcode der Anwendung von innen nach außen geprüft und analysiert wird, während andere Komponenten in Ruhe sind. Grundsätzlich überwacht SAST die Schwachstellen im Quelltext der Anwendung, um problematische Programmiermuster zu identifizieren, die gegen die Best Practices für die Softwareentwicklung verstoßen. Darüber hinaus kann SAST unter Verwendung gängiger Sicherheitsindustriestandards wie OWASP Top Ten und CWE/SANS 25 (gefährlichste Softwarefehler) den Anwendungscode automatisch auf eine Reihe von Schwachstellen testen (what-is-sast, 2022).

Schwachstellen

#### **Cross-Site-Scripting (Webseitenübergreifendes Skripting)**

Bei dieser Cybersicherheitsschwachstelle teilen Angreifende ein manipuliertes Browserskript mit den legitimen Benutzenden und bringen sie dazu, darauf zu klicken, damit die Angreifenden Zugang zu einer Anwendung erhalten. SAST verhindert diese Art von Schwachstelle, indem es die bösartigen Programmcodes überprüft und stoppt.

#### [SQL-Injektion](https://www.wallarm.com/what/structured-query-language-injection-sqli-part-1)

Um Datenbanken zu schädigen, fügen Angreifende einen bösartigen Programmcode in die SQL-Abfrage ein. SAST kann jedes bösartige Element, das in den Quelltext eingeschleust wird, sofort erkennen.

#### [Pufferüberläufe](https://www.wallarm.com/what/buffer-overflow-attack-definition-types-use-by-hackers-part-1)

Wenn eine Anwendung eine große Datenmenge im Puffer speichert, kommt es zu einem Überlauffehler, der die gepufferten Quelltexte beschädigen kann. SAST entschärft dieses Risiko, indem es überprüft, ob die Quelltexte fehlerfrei generiert und vor der Ausführung kontrolliert werden.

#### Angriff auf die Eingabeüberprüfung (input validation attack)

Bei dieser Schwachstelle, die mit SAST leicht erkannt und behoben werden kann, wird eine korrumpierte Eingabe in eine Anwendung eingefügt, um deren Auswirkungen zu sehen.

SAST unterstützt auch die Einhaltung von Datenschutzgesetzen wie dem [Payment Card Industry Data Security Standard](https://www.pcisecuritystandards.org/) (PCI DSS; Schmitt, 2022).

SAST-Tools verhindern Sicherheitsprobleme durch die folgenden Schritte (Eyal Katz, 2021):

1. Informationssammlung: Analyse des Technologiestacks der Anwendung, der wichtigsten Sicherheitsfunktionen und der Erstellungsprozesse.
2. Vorbereitung und Kompilierung: Konfiguration des Quelltextes der Anwendung und der erforderlichen Abhängigkeiten.
3. Scannen des Quelltextes auf Schwachstellen: Automatischer Quelltext-Scan durch integrierte Prozesse.
4. Analyse und Verifizierung: Manuelles Priorisieren der Sicherheitsmängel im Quelltext, um ausnutzbare sicherheitskritische Schwachstellen zu entdecken, nachdem falsch positive Ergebnisse eliminiert wurden.
5. Berichterstattung: Bereitstellung eines detaillierten Berichts über kritische Schwachstellen gemeinsam mit Richtlinien zu deren Behebung.

Static Application Security Testing

Quelle: Reza Vahidnia (2022) basierend auf Eyal Katz (2021)

SAST-Tools, welche die Programmcodes im Ruhezustand scannen, ermöglichen es den Entwickelnden, ihre Anwendung zu testen, ohne funktionale Komponenten auszuführen. Dadurch können Sicherheitsprobleme in späteren Entwicklungsstadien vermieden werden. Diese Tools schützen die Programmcodes vor Sicherheitsproblemen wie der unverschlüsselten Datenübertragung oder der Speicherung von Benutzernamen/Passwörtern im Klartext. Klocwork, Checkmarx, [LGTM.COM](https://lgtm.com/) und [Veracode](https://www.veracode.com/) sind einige der bekanntesten SAST-Tools, die von Softwareentwickelnden verwendet werden (Schmitt, 2022). Die Qualität des Quelltextes kann auch mit Hilfe von Tools wie SonarQube, einer Open-Source-Plattform zur Erkennung von Quelltext-Fehlern in verschiedenen Programmiersprachen, kontinuierlich überprüft werden (sonarsource, n.d.).

Ein geeignetes SAST-Tool wird anhand folgender Kriterien ausgewählt ( Amrita Pathak, 2022):

* Arten von Schwachstellen, die das Tool erkennen kann.
* Programmiersprache der Anwendung.
* Kompatibilität des SAST-Tools mit anderen Entwicklungs-Tools.
* Genauigkeit der Anwendung bei der Erkennung von Sicherheitsproblemen (z. B. die Anzahl der Fehlalarme).

SAST hat einige Vor- und Nachteile, die in der nachstehenden Tabelle aufgeführt sind.

|  |  |
| --- | --- |
| SAST Vor- und Nachteile | |
| **Vorteile** | **Nachteile** |
| * Fehler können bereits in frühen Entwicklungsstadien erkannt werden. * Der genaue Ort des Fehlers wird angezeigt. * Es handelt sich um eine nicht-ausführende Methode. * Für die Automatisierung ist nicht allzu viel Konfiguration erforderlich. | * Die Zahl der falsch-positiven Fälle kann hoch sein. * Es kann sein, dass der falsche Quelltext-Abschnitt markiert wird. * Es handelt sich um ein sprachabhängiges Tool. |

Quelle: Reza Vahidnia (2022) basierend auf (what-is-sast, 2022)

### Fragen zur Selbstkontrolle

1. Bitte erläutern Sie SAST und geben Sie an, in welchen Phasen der Softwareentwicklung es eingesetzt wird.

Static Application Security Testing (SAST) ist eine Scan-Methode oder ein Tool, das Entwickelnden dabei hilft, ihre Quell- oder Assembler-Codes zu überprüfen, bevor sie kompiliert werden, um Sicherheitsschwachstellen in den frühen Entwicklungsphasen zu entdecken.

1. Bitte wählen Sie einen Nachteil von SAST aus.

* Es handelt sich um ein sprachabhängiges Tool.
* Fehler werden bereits in frühen Entwicklungsstadien erkannt.
* Der genaue Ort des Fehlers wird angezeigt.
* Es handelt sich um eine nicht-ausführende Methode.

1. Nennen Sie bitte vier Schwachstellen, die SAST-Tools erkennen können.

[Cross-Site-Scripting](https://www.wallarm.com/what/a7-cross-site-scripting-xss-2017-owasp)

[SQL-Injektion](https://www.wallarm.com/what/structured-query-language-injection-sqli-part-1)

[Pufferüberläufe](https://www.wallarm.com/what/buffer-overflow-attack-definition-types-use-by-hackers-part-1)

Angriff auf die Eingabeüberprüfung

## Dynamisches Testen

Im Gegensatz zu SAST, bei dem die Quelltexte vor dem Kompilieren Zeile für Zeile im Ruhezustand der Anwendung gescannt werden, wird beim Dynamic Application Security Testing (DAST, dynamischer Sicherheitstest von Applikationen) die Anwendung getestet, während die Quelltexte ausgeführt werden. DAST ist ein Black-Box-Ansatz (von außen nach innen), bei dem die Testenden keinen Einblick oder Zugang zu den Quelltexten haben (DAST kann nicht auf bestimmte Codezeilen verweisen, wenn eine Schwachstelle entdeckt wird). Der Ansatz untersucht lediglich die unerwarteten Ergebnisse der Anwendung als Reaktion auf simulierte externe Angriffe. Anhand der Simulationsergebnisse können die Schwachstellen der Anwendung für reale Cyberangriffe ermittelt werden.

DAST kann viele externe Sicherheitsprobleme identifizieren, z. B. die zehn größten OWASP-Schwachstellen, Cross-Site-Scripting, SQL-Injektion und **Path-Traversal**-Angriffe. Aufgrund seiner dynamischen Arbeitsweise ist DAST auch bei der Suche nach Laufzeit-, Authentifizierungs- und Serverkonfigurationsproblemen gegenüber SAST im Vorteil. Außerdem können mit DAST die Sicherheitslücken aufgedeckt werden, die bei der Anmeldung eines bestimmten Clients auftreten.

**Path Traversal**

Eine Sicherheitsbedrohung, die versucht, auf Daten zuzugreifen, die außerhalb des Stammordners des Webs gespeichert sind.

Beachten Sie, dass sich DAST von Penetrationstests (Pentests) unterscheidet. Während beim Pentest versucht wird, Schwachstellen der Anwendung, der Server, der Ports, der Router und der Firewalls mit bekannten Hacking-Methoden auszunutzen, geht es beim DAST hauptsächlich darum, eine laufende Anwendung mit systematischen Methoden zu testen. Um DAST zu implementieren und effektiv zu verwalten, müssen die Sicherheitsexpert:innen die Anwendung sowie die Webserver, Datenbanken, Zugriffskontrolllisten und den Datenfluss der Anwendung genau kennen und verstehen (Murray, 2021).

DAST ist ein leistungsfähiges Tool zum Auffinden von Konfigurationsproblemen in Datenbanken und Servern, die sich auf die Sicherheit von Anwendungen auswirken. Darüber hinaus kann DAST Verschlüsselungs- und Authentifizierungsprobleme erkennen, die einen unbefugten Zugriff ermöglichen. Eine solche Fähigkeit gibt es bei SAST nicht. DAST ist auch in der Lage, die gesamte IT-Infrastruktur und das Netzwerk zu testen, indem die mit der Anwendung verbundenen Netzwerke, APIs und Webdienste untersucht werden (Schmitt, 2022). [Invicti](https://www.invicti.com/product/) und [Probely+](https://probely.com/enterprise/) sind zwei sehr bekannte DAST-Tools.

DAST kann auf allen Anwendungen laufen, da es nicht von bestimmten Technologien, Plattformen oder Sprachen abhängig ist. DAST wurde von OWASP getestet und hat im Vergleich zu anderen Tools zum Testen der Anwendungssicherheit eine geringere Fehlalarmquote. Da DAST die Anwendung von außen angreift und prüft, gilt es als perfektes Werkzeug zur Erkennung von Konfigurationsproblemen, die mit anderen Sicherheitstools nicht so leicht zu finden sind.

DAST ist zwar ein hervorragendes Instrument zum Aufspüren von Sicherheitsschwachstellen, hat aber auch seine Grenzen. Einer der Hauptnachteile von DAST ist seine geringe Skalierbarkeit, da es in hohem Maße von Sicherheitsexpert:innen abhängt, die effektive Tests entwickeln. Darüber hinaus ist DAST nicht in der Lage, die Anwendungsentwickelnden auf die problematischen Teile des Quelltextes hinzuweisen, da es dorthinein keinen Einblick hat. Es bietet also für sich allein keine umfassende Sicherheitsabdeckung. Ein weiterer Nachteil von DAST ist seine geringe Geschwindigkeit, da DAST-Scans zum Testen einer Anwendung sogar mehrere Tage dauern können. Außerdem findet DAST Sicherheitsschwachstellen in der Regel erst in späten Entwicklungsphasen, was deren Behebung teurer und zeitaufwändiger macht. Die Vor- und Nachteile von DAST sind in der nachstehenden Tabelle zusammengefasst.

|  |  |
| --- | --- |
| SAST Vor- und Nachteile | |
| **Vorteile** | **Nachteile** |
| * Unabhängig von Technologien * Wenige Fehlalarme * Identifizierung von Konfigurationsproblemen | * Geringe Skalierbarkeit * Kein Einblick in den Quelltext * Langsam und zeitaufwändig |

Quelle: Reza Vahidnia (2022) basierend auf Murray (2021)

Ein geeignetes DAST-Tool wird in der Regel anhand der folgenden Kriterien ausgewählt **Ungültige Quelle angegeben.**:

* Arten von Schwachstellen, die das Tool erkennen kann.
* Automatisierungsgrad des DAST-Tools für die Planung und Durchführung der Scans.
* Kompatibilität des DAST-Tools mit anderen existierenden Tools.
* Anpassungsmöglichkeiten, die das Tool für die Konfiguration eines bestimmten Testfalls bietet.

Um eine größere Angriffsfläche zu berücksichtigen, sammeln DAST-Tools zunächst so viele Informationen wie möglich über die Anwendung. Anschließend scannt das Tool die Anwendung aktiv und testet die Schwachstellen für z. B. SQL-Injektionen, indem es verschiedene Attacken auf die zuvor gefundenen Zielorte ausführt. Mit den DAST-Tools können Entwickelnde und Sicherheitsexpert:innen auch benutzerdefinierte Angriffsszenarien für die Cybersicherheit erstellen. Sobald eine Schwachstelle durch das DAST-Tool erkannt wurde, hilft es bei der Behebung des Problems, indem es Informationen über die Schwachstelle wie Typ, Schweregrad und URL liefert (Amrita Pathak, 2022).

Der Hauptunterschied zwischen statischem und dynamischem Testen besteht in der Art und Weise, wie die Sicherheitstests durchführt werden. Während SAST die Anwendung im Ruhezustand testet, prüft DAST sie, während der Quelltext ausgeführt wird. Die nachstehende Abbildung veranschaulicht die Unterschiede zwischen diesen beiden Ansätzen zur Prüfung der Anwendungssicherheit.

SAST versus DAST

Grafik in der Grafikdatei

Quelle: Reza Vahidnia (2022) basierend auf sast-vs-dast (2022)

### Fragen zur Selbstkontrolle

1. Bitte erklären Sie, warum DAST keine Korrekturmaßnahmen empfehlen kann.

Da DAST keinen Einblick in den Quellcode hat, kann es die genaue Stelle oder Zeile des Programmcodes nicht ausfindig machen, die zu der Sicherheitslücke führt.

## 3.4 DevSecOps

In der traditionellen Softwareentwicklung wurden Sicherheitsmaßnahmen und -praktiken in der Regel erst im Nachhinein erwogen und erst in den fortgeschrittenen Phasen des SDLC berücksichtigt und implementiert (und nicht bereits in den frühen Phasen des Software-Lebenszyklus). Dieser Ansatz funktioniert jedoch nicht in modernen Entwicklungssystemen, in denen es kürzere und häufigere Iterationen von Anwendungen gibt und die Sicherheitsbedrohungen ausgefeilter sind.

DevSecOps, das Entwicklung (development), Sicherheit (security) und Betrieb (operation) vereint, ist ein Entwicklungsansatz, bei dem Sicherheitsinitiativen in jede Phase des Softwareentwicklungs-Lebenszyklus integriert werden. Mit anderen Worten: DevSecOps bedeutet, dass die Sicherheit der Infrastruktur und der Anwendungen von Beginn des Projekts an berücksichtigt wird.

**CI/CD Pipeline**

Eine Reihe von notwendigen Schritten zur Bereitstellung einer neuen Softwareversion.

DevSecOps, das Sicherheitspraktiken in die **CI/CD-Pipeline** (Continuous Integration/Continuous Delivery-Pipeline) einfließen lässt, führt zur Bereitstellung sicherer und robuster Anwendungen. Dies ermöglicht Softwareentwickelnden die zügige Lösung vieler der anspruchsvollsten Sicherheitsprobleme (devsecops, 2022).

### Vorteile von DevSecOps

Der DevSecOps-Ansatz bringt viele Vorteile für Unternehmen mit sich, darunter die folgenden. **Ungültige Quelle angegeben**

#### Verbesserte Anwendungssicherheit

Mit DevSecOps werden die Sicherheitsbedrohungen bereits in den frühen Phasen des Entwicklungslebenszyklus entschärft. Automatisierte Sicherheitstools in DevSecOps ermöglichen es den Entwickelnden, die Programmcodes in jeder Phase des Entwicklungslebenszyklus zu überprüfen, zu auditieren und zu kontrollieren, ohne die Geschwindigkeit zu beeinträchtigen. Auf diese Weise wird sichergestellt, dass die Anwendung kein Sicherheitskriterium verletzt, und falls doch, können die Sicherheitsexpert:innen und Softwareentwickelnden Lösungen vorschlagen, um das Problem auf Quelltext-Ebene zu beheben.

#### Teamübergreifende Zuständigkeit

Im Gegensatz zu herkömmlichen Entwicklungsmethoden, bei denen die verschiedenen Teams in getrennten Abteilungen arbeiten, kooperieren bei DevSecOps die Entwicklungs-, Sicherheits- und Betriebsteams bereits in den frühen Phasen des Entwicklungslebenszyklus effektiv.

#### Optimierung der Bereitstellung von Anwendungen

Beim DevSecOps-Ansatz wird die Sicherheit durch automatisierte Maßnahmen während der Entwicklung der Anwendung verbessert, um Verzögerungen bei der Produktbereitstellung zu vermeiden.

#### Begrenzung von Sicherheitsschwachstellen

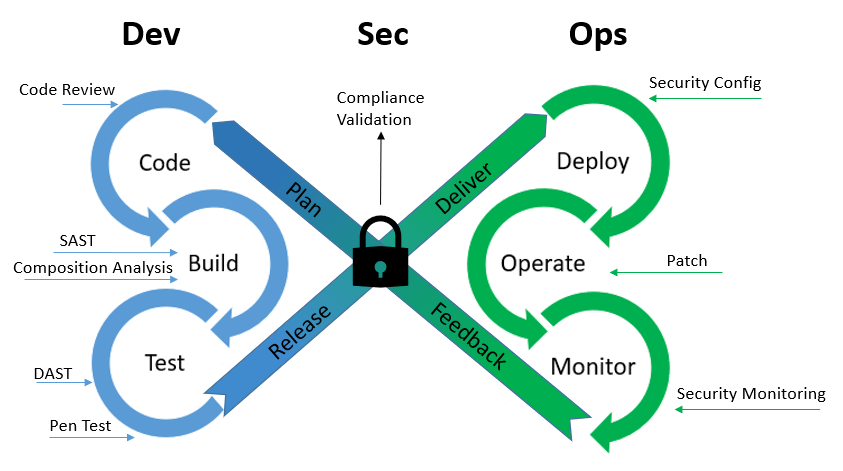
DevSecOps schafft einen straffen, agilen Entwicklungsprozess, in dem die Sicherheitsteams nicht nur Schwachstellen aufspüren, um Risiken zu mindern, sondern dem Entwicklungsteam auch nützliche Erkenntnisse liefern, um die entdeckten Sicherheitsprobleme schnell zu beheben.

DevSecOps bringt auch viele Vorteile für verschiedene Industriesegmente und Branchen mit sich. Beispielsweise wird das Risiko der Ausnutzung von Schwachstellen in Regierungs-, Gesundheits- oder Finanzanwendungen, um Zugang zu sensiblen Informationen zu erhalten, durch DevSecOps erheblich reduziert.

### DevSecOps Lebenszyklus

DevSecOps hat den traditionellen Softwareentwicklungsansatz, bei dem die Lieferung in einem Wasserfallprozess erfolgte, durch automatisierte, kleinere und häufigere Lieferungen mit vielen Feedbackschleifen zur schnellen und kontinuierlichen Verbesserung ersetzt. Die folgende Abbildung veranschaulicht den DevSecOps-Lebenszyklus, bei dem Sicherheitsaspekte in jede Phase eingebettet sind.

DevSecOps Software-Lebenszyklus



Quelle: Reza Vahidnia (2022) basierend auf devsecops (2022)

In der Entwicklungsphase von DevSecOps werden zunächst die Bedrohungsmodelle definiert, verschiedene Ansätze zur Abschwächung der Datenverletzungsrisiken untersucht und lokale und nationale Sicherheitsrichtlinien recherchiert. Anschließend werden die Open-Source-Bibliotheken inspiziert und eine Quelltextüberprüfung in die Entwicklungsprozesse eingebettet, sodass die in der Planungsphase festgelegten Sicherheitsanforderungen erfüllt werden. Nachdem die Sicherheitsanforderungen und ihre Akzeptanzkriterien definiert sind und der Bauplan vorliegt, wird SAST zur Schwachstellenbehebung durchgeführt. Sobald die Programmcodes ausgeführt werden können, werden während der Ausführung DAST und Penetrationstests durchgeführt, um die Anwendung in einer dynamischen Umgebung zu testen, indem externe Angriffe simuliert werden.

**Patch**

Eine Software, die Sicherheitsschwachstellen durch Fehlerkorrektur im Quelltext behebt.

In der Betriebsphase umfassen die Sicherheitsüberlegungen die Aufklärung der Benutzenden über die Sicherheitsanforderungen, die Überwachung von Schwachstellen und die Kontrolle des Benutzerzugangs sowie die Verwaltung von Sicherheits**patches**.

### DevSecOps-Säulen

Die erfolgreiche Implementierung von DevSecOps stützt sich auf drei Säulen: Menschen, Prozesse und Technologien.

* **Menschen:** Die Implementierung einer effektiven DevSecOps-Umgebung ist ohne die Unterstützung der obersten Führungsebene eines Unternehmens nicht möglich.
* **Prozesse:** Die Entwicklung unterschiedlicher Software erfordert unterschiedliche Managementprozesse, die aus vielen Komponenten bestehen, dazu gehören auch die Dokumente zur Standardisierung des Arbeitsablaufs. Diese Prozesse hängen von vielen Faktoren ab, darunter die Komplexität, die Architektur und der Reifegrad des Systems.
* **Technologien:** DevSecOps-Prozesse werden mit Hilfe verschiedener Technologien wie Automatisierungs- und Konfigurationsmanagement, Security-as-Code, automatisierte Compliance-Scans und Host-Härtung durchgeführt.

DevSecOps-Säulen

Quelle: Reza Vahidnia (2022)

### DevOps versus DevSecOps

DevOps, das die Softwareentwicklung (Dev) und den IT-Betrieb (Ops) miteinander verbindet, schafft eine Zusammenarbeit zwischen Programmierer:innen und Systemadministrator:innen, um den SDLC zu verkürzen und eine kontinuierliche Bereitstellung mit hoher Softwarequalität zu gewährleisten. DevSecOps, das eine Erweiterung von DevOps ist, betont die Sicherheit in jeder Phase des SDLC.

DevOps versus DevSecOps

**Runtime Application Self-Protection (RASP)**

Ein Sicherheitsmechanismus, der zur Laufzeit eingesetzt wird, um Angriffe zu erkennen und zu verhindern, indem er Informationen aus dem Inneren der laufenden Software nutzt.

Quelle: Reza Vahidnia (2022) basierend auf **Ungültige Quelle angegeben.**

Für den Übergang von DevOps zu DevSecOps sind bestimmte Technologien erforderlich, um die Sicherheitsmaßnahmen in verschiedenen Phasen des SDLC zu automatisieren. Dazu gehören: SAST (Erkennung von Sicherheitsschwachstellen in der Codierungsphase), DAST (Black-Box-Test zur Ermittlung von Schwachstellen, während der Code in der Testphase läuft), **Runtime Application Self-Protection (RASP)**, und Interactive Application Security Testing ([IAST](http://www.quotium.com/resources/interactive-application-security-testing/)) (analysiert die Anwendung, um bestimmte Ereignisse zu finden, die zu einer Schwachstelle führen können), Software Composition Analysis (SCA) (erkennt Schwachstellen in Open-Source-Komponenten).

### Fragen zur Selbstkontrolle

1. Bitte erläutern Sie, wie DevSecOps zur Bereitstellung sicherer und robuster Anwendungen führt.

DevSecOps, das Entwicklung (development), Sicherheit (security) und Betrieb (operation) vereint, ist ein Entwicklungsansatz, bei dem Sicherheitsinitiativen in jede Phase des Softwareentwicklungs-Lebenszyklus integriert werden. DevSecOps lässt Sicherheitspraktiken in die (CI/CD)-Pipeline einfließen und führt daher zur Bereitstellung sicherer und robuster Anwendungen. Dies ermöglicht Softwareentwickelnden die zügige Lösung vieler der anspruchsvollsten Sicherheitsprobleme.

1. Bitte wählen Sie aus, in welcher Phase von DevSecOps, SAST durchgeführt wird.

* Einsatz
* Test
* Erstellung
* Überwachung

Zusammenfassung

Beim Konzept des „Security by Design“ wird Sicherheit als ein wesentliches Ziel in allen Phasen des Softwareentwicklungs-Lebenszyklus betrachtet. Dieser Ansatz führt dazu, dass Sicherheitsschwachstellen im Programmcode bereits in den frühen Entwicklungsphasen erkannt werden. Infolgedessen können Sicherheitsprobleme billiger und einfacher angegangen werden als bei traditionellen Softwareentwicklungsmethoden, bei denen Sicherheit als Engpass angesehen und erst in späten Entwicklungsphasen in Angriff genommen wurde.

DevSecOps vereint Entwicklung, Sicherheit und Betrieb und integriert Sicherheitsinitiativen in jede Phase des Lebenszyklus der Softwareentwicklung. Es lässt Sicherheitspraktiken in die (CI/CD)-Pipeline einfließen und führt daher zur Bereitstellung sicherer und robuster Anwendungen. Dies ermöglicht es Softwareentwickelnden, viele der anspruchsvollsten Sicherheitsprobleme zügig zu lösen. SAST und DAST sind zwei leistungsstarke Tools, die im Rahmen von DevSecOps eingesetzt werden, um die Programmcodes auf Sicherheitsrisiken zu prüfen und diese in den frühen Phasen der Entwicklung zu beheben. Während SAST die Quelltexte in Ruhe vor der Kompilierung testet, prüft DAST den Quelltext während der Ausführung, indem es externe Bedrohungen für die Anwendung simuliert.

# Lektion 4 – Gerätesicherung im Internet der Dinge

**Lernziele**

Nach dem Abschluss dieser Lektion werden Sie...

... die Sicherheitsrisiken identifizieren können, von denen IoT-Geräte bedroht werden.

... die Sicherheitsprobleme und Risiken für jede Angriffsschicht von IoT-Geräten auflisten können.

... die verschiedenen Sicherheitstechniken erläutern können, die verwendet werden, um IoT-Geräte zu schützen.

... erklären können, wie Paketverschlüsselung den Datentransfer zwischen IoT-Geräten sichern kann.

# 4. Gerätesicherung im Internet der Dinge

## Einführung

Die enorme Anzahl von IoT-Geräten von verschiedenen Herstellern, die von zahlreichen Händlern verkauft und in den unterschiedlichsten Branchen und Industriebereichen verwendet werden, bieten eine riesige Angriffsfläche für böswillig Agierende, Hacker:innen und Wettbewerbsunternehmen. Sicherheitsverletzungen bei IoT-Geräten bedrohen die Sicherheit von Individuen, schädigen Unternehmen, das Kundenvertrauen und den Ruf von Firmen.

Regulierungsbehörden fordern möglicherweise Bußgelder von Unternehmen, wenn Sicherheitsverletzungen gegen Verordnungen verstoßen. Der Verstoß gegen die Verordnungen des Health Insurance Portability and Accountability Act (HIPAA) – ein US-Bundesgesetz zum Schutz vertraulicher Gesundheitsdaten vor Weitergabe ohne Zustimmung der Patient:innen – führt beispielsweise dazu, dass Firmen Bußgelder von bis zu 50.000 $ zahlen müssen (IoT Devices Security, 2017). Ein weiteres Beispiel: Jeder Regelverstoß gegen den Payment Card Industry Data Security Standard (PCI DSS) führt dazu, dass Kreditkartenunternehmen ihre Geschäftstätigkeit einstellen müssen, denn ohne PCI-Erlaubnis darf ein Unternehmen keine Kartenzahlungen verarbeiten.

Die meisten herkömmlichen Sicherheitsmechanismen, die auf informationstechnischen Geräten (z. B. Laptops und Smartphones) eingesetzt werden, sind nicht auf einfache und kostengünstige IoT-Geräte übertragbar. IoT-Geräte brauchen andere Sicherheitsansätze, um Cyberangriffen zu begegnen, weil ihre Sicherheitsrisiken andere sind als bei traditionellen IT-Netzwerken.

## 4.1 Sicherheitsrisiken

IoT-Geräte sind verlockende und manchmal einfach zu erreichende Ziele für böswillige Nutzende und Angreifende, da die für PCs und Smartphones üblichen Sicherheitstechniken und Mechanismen nicht auf IoT-Geräte angewendet werden können, und zwar aus den folgenden Gründen (IoT Devices Security, 2017):

1. **Begrenzte Ressourcen:** Die meisten preiswerten IoT-Geräte erfüllen nicht die Anforderungen an Speicher, Batterie und Rechenleistung, um herkömmliche Sicherheitsmechanismen umzusetzen. IoT-Geräte mit geringem Speicherplatz erlauben beispielsweise keine Patch-Mechanismen zur Behebung häufiger Schwachstellen und Gefährdungen (CVEs, Common Vulnerabilities and Exposures).
2. **Wert der Daten:** Einige Betriebe nehmen die IoT-Sicherheit nicht ernst, da sie der Meinung sind, dass ihre Daten außerhalb des Unternehmens nur einen geringen Wert haben. Doch allein das Hacken ihrer IoT-Geräte durch Konkurrenten, selbst wenn diese die gewonnenen Daten nicht wirklich nutzen, kann den Ruf des Unternehmens ruinieren.
3. **Verfügbare Tools:** Es gibt viele leicht verfügbare Tools und Ressourcen für das Hacken von IoT-Geräten. Metasploit und Maltego sind zwei der bekanntesten IoT-Hacking-Tools. Ersteres ist ein Open-Source-Tool, das für Penetrationstests verwendet wird und mit dem sich IoT-Geräte aus der Ferne sichern lassen, nachdem man sich Zugang verschafft und die Software kostenlos angepasst hat. Letzteres ist ebenfalls ein flexibles Open-Source-Tool, das zur Sammlung von Daten für Footprinting, zu Spionagezwecken, für Verbindungsanalysen und Data Mining verwendet wird.
4. **Drahtlose Verbindungen:** Die meisten IoT-Geräte benutzen drahtlose Verbindungen, um ihre Daten zur Cloud zu übertragen. Außerdem kann die Firmware aus der Ferne aktualisiert und konfiguriert werden.Daher brauchen Hacker:innen keinen physischen Zugang zu den Ports der IoT-Geräte.

**Transport Layer Security (TLS)**

Ein Verschlüsselungsprotokoll, das eine gesicherte Kommunikation für Internetverbindungen auf Anwendungsebene ermöglicht.

1. **Einfache Schnittstellen:** Die einfachen Sicherheitsalarme preiswerter IoT-Geräte, bei denen es sich um eine blinkende Leuchtdiode (LED) oder einen piepsenden Summer handeln kann, können übersehen werden, da sie leicht mit anderen Alarmen von Kontrollfunktionen verwechselbar sind.
2. **Hartverdrahtete Ports:** Diese Ports bieten Angreifenden offene Türen, um IoT-Geräte zu kompromittieren.

Im Gegensatz zu PCs und Smartphones können IoT-Geräte nicht einfach von der Implementierung eines starken Passworts über eine **Transport-Layer-Security**- Verbindung (**TLS**, Transportschichtsicherheit) profitieren. Auch wenn einige Sicherheitsangriffe, wie Verteilter Denial-of-Service (Distributed DoS, DDoS) auf die Server und nicht unbedingt direkt auf die IoT-Geräte abzielen, verursachen sie dennoch Probleme für die Geräte, da sie deren Akkus entleeren und folglich die Wartungskosten der Unternehmen erhöhen.

Das Fehlen von Security by Design sowie schlechte Konfiguration von IoT-Geräten aus Gründen der Kundenfreundlichkeit sind zwei wichtige Faktoren, die es Hacker:innen ermöglichen, die Geräte zu manipulieren. Ersteres führt zu mehr Schwachstellen und letzteres möglicherweise zu schwachen Zugangsberechtigungen.

Im Wesentlichen gibt es vier Arten von Sicherheitsrisiken im Zusammenhang mit IoT-Geräten. Diese Risiken sind in der nachstehenden Abbildung dargestellt (IoT Devices Security, 2017).

Sicherheitsrisiken für IoT-Geräte



Quelle: Reza Vahidnia (2022) basierend auf IoT Devices Security (2017)

### Arten von Sicherheitsrisiken

#### Vertraulichkeit

Böswillig Agierende können sich Zugang zu den Daten im eigentlichen IoT-Gerät verschaffen und diese einsehen, ändern oder die Gerätefirmware stehlen/klonen. Um sensible IoT-Daten vertraulich zu halten, sollten auf den IoT-Geräten fortschrittliche Datenschutzmechanismen implementiert werden.

Ein Beispiel für eine Datenschutzbedrohung ist der TRENDnet-Webcam-Hack, bei dem der IP-Kamerahersteller TRENDnet die Zugangsdaten seiner Kundschaft im Klartext gespeichert und unverschlüsselt über das Internet verschickt hat. Der Fehler in der Software ermöglichte es Hacker:innen außerdem, auf die Video- und Audiodaten der Kameras zuzugreifen, weil sie die IP-Adressen hatten (Dian, 2022). Dies zeigt, dass Hersteller von IoT-Geräten Sicherheitsmaßnahmen in ihre Geräte einbauen müssen, um Sicherheitsverletzungen zu verhindern, während die Nutzenden die Sicherheitsparameter des Geräts entsprechend ihrer Anwendung richtig konfigurieren sollten.

#### Datenintegrität

Wenn böswillig Agierende nicht autorisierte Daten einführen oder die IoT-Daten verändern, um die Kontrolle über die Geräte zu übernehmen, wird die Datenintegrität verletzt. So könnten Hacker:innen beispielsweise die IoT-Daten eines intelligenten Schlosses ändern, um es jederzeit aufschließen zu können.

#### Diebstahl von Dienstleistungen

Böswillig Agierende können Schwachstellen wie Authentifizierungsschwächen oder -fehler nutzen, um unbefugten Geräten den Zugriff auf IoT-Daten oder -Dienste zu ermöglichen. Dadurch ist es z. B. möglich, dass ohne Autorisation ein Upgrade freigeschaltet wird.

#### Verfügbarkeit

Eine Bedrohung der Verfügbarkeit kann auftreten, wenn Angreifende den Betrieb eines IoT-Systems oder -Geräts unterbrechen. Die Angreifenden können möglicherweise die Geschwindigkeit oder Kapazität des IoT-Geräts herunterfahren oder verringern, indem sie das Netzwerk mit feindlichem Datenverkehr überfluten. Bei dieser Art von Angriff, die als Denial-of-Service (DoS) bezeichnet wird, werden IoT-Geräte manipuliert und angewiesen, das Zielnetzwerk zu überlasten (Dian, 2022).

Eine andere Art von Bedrohung der Verfügbarkeit ist der so genannte Denial-of-Sleep-Angriff (DoSA, Schlafentzugsangriff), bei dem der Angreifende ein gefälschtes Gerät verwendet, um ständig Nachrichten an legitime IoT-Geräte zu senden, damit diese zwischen den Übertragungsintervallen nicht in den Schlafmodus wechseln. Der Zweck von DoSA besteht darin, den Stromverbrauch der IoT-Geräte in der Reichweite des gefälschten Geräts zu erhöhen, ihre Akkulaufzeit zu verkürzen und sie schließlich unerreichbar zu machen.

### Angriffsebenen eines IoT-Geräts

Aus der Sicherheitsperspektive betrachtet, hat ein IoT-Gerät mehrere mögliche Angriffsebenen. Dazu gehören Hardware, Firmware, Betriebssystem, Anwendung, Web-Interface, Protokolle und Richtlinien – jede Angriffsebene hat ihre eigenen Sicherheitsprobleme und damit verbundenen Risiken.

Möglicherweise Grafik

#### Hardware

**Inter-Integrated Circuit (I2C)**

Ein Protokoll, das die Kommunikation mehrerer Sensoren mit einem Steuergerät ermöglicht.

#### Auf der physischen Ebene der Hauptplatine können Angreifende nach Hardware-Debug-Ports wie Joint Test Action Group (JTAG) oder Kommunikationsports, z. B. Inter-Integrated Circuit (I2C), suchen.

#### Firmware

#### In dieser Sicherheitsebene versuchen Hacker:innen, versteckte Backdoors, hardkodierte Passwörter und andere Sicherheitsschwachstellen in der Firmware zu finden. Sie versuchen, diese Passwörter zu erraten, um auf das System zuzugreifen. Probleme mit Zugangsdaten, Backdoor-Probleme, nicht gepatchte Firmware, Pufferüberlaufprobleme und die Ausweitung von Berechtigungen sind einige der Sicherheitsrisiken auf der Firmware-Angriffsebene.

#### Betriebssystem und Anwendung

Auf dieser Ebene suchen Hacker:innen nach Einfallspunkten in Form von Betriebssystem- und Anwendungsfehlern. Ein Beispiel für verwendete Betriebssysteme ist FreeRTOS, ein Echtzeitbetriebsystem-Kernel für eingebettete Geräte. Es ist zu beachten, dass einige IoT-Systeme nicht unbedingt über ein Betriebssystem verfügen und stattdessen alle Funktionen direkt auf der Mikrocontroller-Einheit implementiert sind. In IoT-Systemen mit Betriebssystemen können Pufferüberläufe (Stack, Heap und Integer) Angreifenden die Kontrolle über das System ermöglichen.

#### Web-Interface

Hacker:innen können beim Web-Interface des IoT-Geräts nach Programmierfehlern suchen und so an sensible Daten wie die interne IP-Adresse und die Konfiguration der IoT-Geräte gelangen. Zu den Sicherheitsrisiken auf dieser Angriffsebene gehören die SQL-Injektion, Pufferüberläufe, Cross-Site-Scripting (XSS), Cross-Site-Request-Forgery (CSRF), die Benutzung von Standard- oder Beispielseiten und die Ausweitung von Berechtigungen.

#### Protokoll

**ZigBee**

Eine stromsparende Kommunikationstechnologie, die sich für Smart-Home-Anwendungen eignet.

Angriffe auf die Sicherheit können Schwachstellen in folgenden Kommunikationsprotokollen ausnutzen: Zugangstechnologien mit geringer Reichweite (z. B. **ZigBee**), Protokolle mit großer Reichweite einschließlich zellularer IoT-Technologien (z. B. NB-IoT und LTE-M) und nichtzellulare Low-Power-Wide-Area-Technologien (LPWA, z. B., LoRAWAN und SigFox). Dabei werden möglicherweise Gerätefunktionen durch Ausschöpfen der Übertragungsbandbreite deaktiviert, die Authentifizierung durch die Wiedergabe gestohlener Daten umgangen, Hijacking-Sitzungen zum Senden gefälschter Informationen initiiert und Daten durch Man-in-the-Middle-Angriffe gestohlen.

#### Richtlinien

Böswillig Agierende können Richtlinien angreifen, die sensible Daten oder die Einstellungen enthalten, welche ihnen das Öffnen des Geräts außerhalb des lokalen Netzwerks ermöglichen.

### Einsatzfall Smart Home

Als Beispiel-Einsatzfall wollen wir ein Smart Home betrachten, um die Sicherheitsprobleme verschiedener intelligenter Geräte zu untersuchen und die Risiken eines Hackerangriffs auf diese Geräte zu erkennen. Die nachstehende Tabelle enthält eine Liste von IoT-Geräten in einem Smart Home und die Aktionen, die Angreifende durchführen könnten, wenn diese Geräte kompromittiert wurden.

Smart-Home-Geräte und mögliche Sicherheitsrisiken

|  |  |
| --- | --- |
|  | |
| **Intelligentes Gerät** | **Sicherheitsrisiko** |
| Sprachgesteuertes  Gerät zur  Heimautomatisierung | * Verursacht Belästigungen durch das Abspielen bösartiger Sprachbefehle zu unerwünschten Zeiten * Bestellung unerwünschter Waren durch gefälschte Sprachbefehle * Diebstahl von Sprachdaten zur Verwendung als Anmeldetaten für andere sprachgesteuerte Systeme |
| Intelligenter Kühlschrank | * Automatische Bestellung nicht benötigter Lebensmittel * Verändern der eingestellten Temperatur, um Lebensmittel zu verderben * Ändern des Verfallsdatums, um vorzutäuschen, dass die Lebensmittel frisch sind |
| Intelligentes Schloss | * Absichtlich für Einbrecher:innen aufschließen * Rechtmäßige Bewohnende aussperren * Ändern des Schließpassworts * Anschalten der Alarmanlage, obwohl niemand eindringt oder einbricht |
| Intelligente Beleuchtung | * Zu ungewollten Zeiten das Licht ein- oder ausschalten * Überlastung des Stromnetzes durch Einschalten aller Lampen * Blinklicht zum Stören der Bewohnenden |
| Intelligente Kaffeemaschine | * Unterbrechen des Brühvorgangs * Maschine komplett deaktivieren * Kontinuierlich brühen, obwohl gar keine Kaffeebohnen mehr vorhanden sind |
| Smart Home Gateway | * Herunterladen von Schadsoftware durch Verbindung mit einer bösartigen oder gefälschten URL * Zugang zu Anmeldedaten oder persönlich identifizierbaren Informationen * Kontrolle über die an das Gateway angeschlossenen Geräte erlangen * Umleiten von Verbindungen zu versteckten bösartigen Verhaltensweisen durch Blockieren oder Modifizieren |

Quelle: Reza Vahidnia (2022) basierend auf Ohang (2019)

**Universelles Plug-and-Play (UPnP)**

Ein Protokoll, das es IoT-Geräten ermöglicht, andere Geräte automatisch zu erkennen und sich mit ihnen zu verbinden.

Einige der oben aufgeführten Sicherheitsrisiken mögen auf den ersten Blick harmlos erscheinen. Wenn jedoch nur ein einziges IoT-Gerät bei der Sicherheitsbetrachtung übersehen wird, besteht die Gefahr einer Kombination schwerwiegender Sicherheitsbedrohungen, falls Hacker:innen die Schwachstelle des Geräts ausnutzen.

Beispielsweise ist es zunächst schwer vorstellbar, dass eine nicht gesicherte intelligente Kaffeemaschine ein Sicherheitsrisiko für das gesamte Smart Home darstellt, wenn sie kompromittiert wird. Die **universelle Plug-and-Play-Funktion (UPnP-Funktion)** der intelligenten Kaffeemaschine kann jedoch automatisch eine Verbindung zum Internet über den Smart Home Router herstellen. Böswillig Agierende können die intelligente Kaffeemaschine nun leicht manipulieren und nutzen, um sich mit dem Layout des Smart Home vertraut zu machen und dann andere mit dem Heimnetzwerk verbundene intelligente Geräte zu beeinträchtigen. Folglich können Hacker:innen die Bewohnenden in die Irre führen, indem sie falsche Informationen über intelligente Geräte senden, die Bewohnenden über die kompromittierten IP-Kameras und sprachgesteuerten Hausautomatisierungsgeräte überwachen, falsche Alarme auslösen, die intelligenten Schlösser entriegeln, damit Unbefugte das Haus betreten können, während sie die intelligenten Glühbirnen und das Alarmsystem ausschalten. Darüber hinaus können sich Hacker:innen Zugang zu den Smartwatches der Bewohnenden verschaffen, um sie auszuspionieren, ihre Aktivitäten zu überwachen und ihren Standort jederzeit in Echtzeit zu überprüfen.

### Fragen zur Selbstkontrolle

1. Bitte erläutern Sie die Sicherheitsrisiken auf der Protokollebene eines IoT-Geräts.

Angreifende können nach Schwachstellen in den Kommunikationsprotokollen wie Wi-Fi suchen, um Gerätefunktionen durch Ausschöpfung der Übertragungsbandbreite zu deaktivieren, um die Authentifizierung durch Wiedergabe gestohlener Daten zu umgehen, um Hijacking-Sitzungen zum Senden gefälschter Informationen zu initiieren und durch Man-in-the-Middle-Angriffe Daten zu stehlen.

1. Bitte wählen Sie aus, in welcher Angriffsebene eines IoT-Geräts Hacker:innen Gerätefunktionen durch Überlastung der Übertragungsbandbreite deaktivieren können.

* Protokoll-Ebene
* Hardware-Ebene
* Web-Interface-Ebene
* Firmware-Ebene

1. Bitte nennen Sie fünf Sicherheitsprobleme der Firmware-Angriffsebene eines IoT-Geräts.

Probleme mit Zugangsdaten

Probleme mit versteckten Backdoors

Ungepatchte Firmware

Probleme mit Pufferüberläufen

Ausweitung von Berechtigungen

1. Eine Art von Sicherheitsrisiko bei IoT-Geräten ist die Beeinträchtigung der Verfügbarkeit. Bitte erklären Sie, inwiefern ein DoSA eine Bedrohung für die Verfügbarkeit darstellt.

Beim Denial-of-Sleep-Angriff (DoSA, Schlafentzugsangriff) verwenden die Angreifenden ein gefälschtes Gerät, um ständig Nachrichten an legitime IoT-Geräte zu senden, damit diese zwischen den Übertragungsintervallen nicht in den Schlafmodus wechseln. Der Zweck von DoSA besteht darin, den Stromverbrauch der IoT-Geräte in der Reichweite des gefälschten Geräts zu erhöhen, ihre Akkulaufzeit zu verkürzen und sie schließlich unerreichbar zu machen.

## 4.2 Design-Ziele

Jeden Tag testen Cyberangreifende innovative neue Methoden, um IoT-Systeme zu attackieren. Selbst die fortschrittlichsten IoT-Geräte mit ausgefeilten Sicherheitsmaßnahmen sind anfällig für Sicherheitsbedrohungen und können gehackt werden. Das heißt, egal wie viel Geld, Zeit und Mühe in die Sicherung eines IoT-Geräts gesteckt werden, so ist es immer noch nicht perfekt gegen erfahrene böswillig agierende Personen geschützt. Daher ist es von entscheidender Bedeutung, die Beeinträchtigung von IoT-Geräten für Angreifende so unwirtschaftlich wie möglich zu machen. Mit anderen Worten: Angreifende hören möglicherweise auf, ein IoT-System anzugreifen, wenn sie das Gefühl haben, dass sich die Kosten und der Aufwand zum Hacken des Systems nicht lohnen. Die Secure Design Best Practices Guidelines (BPGs) der IoTSF (IoT Security Foundation) geben wichtige Empfehlungen für die Sicherheit von IoT-Produkten und -Systemen, einschließlich physischer Geräte, Betriebssysteme, Anwendungen, Software-Updates und Netzwerkverbindungen. Im Folgenden finden Sie zum Beispiel eine Liste von Richtlinien zum physischen Schutz von IoT-Geräten (Secure Design: Best Practices Guide, 2019):

* Entfernen oder Deaktivieren der Test- und Verwaltungsschnittstellen.
* Deaktivieren oder Sperren der Testzugänge auf den Produktionseinheiten.
* Sicherstellen, dass die erforderlichen Administrationsports über wirksame Zugangskontrollen verfügen, wie z. B. eine strenge Verwaltung der Anmeldeinformationen, eingeschränkte Ports und sichere Protokolle.
* Verwendung von epoxidharzbeschichteten Chips für Leiterplatten, Verkapselung und Verbergen von Daten- und Adressleitungen unter diesen Komponenten, um die Schaltkreise des Geräts physisch unzugänglich für Manipulationen zu machen.
* Verwendung sicherer Schutzgehäuse für exponierte Geräte.
* Sicherstellen der Manipulationssicherheit der Geräte.
* Verwendung aktiver Maskierung oder Abschirmung zum Schutz vor Seitenkanalangriffen.

Sicherheitsangriffe lassen sich anhand ihrer Kosten, der verwendeten Ausrüstung und der Art der Angreifenden wie folgt kategorisieren.

Kategorien von Sicherheitsangriffen auf Geräte

Quelle: Reza Vahidnia (2022) basierend auf IoT Devices Security (2017)

Der erforderliche Aufwand an Zeit, Mühe und Investitionen in die Sicherheit wird in der Regel durch die wirtschaftlichen Kosten und Vorteile der Gerätesicherung bestimmt, die wiederum vom Wert des Geräts und seiner Daten abhängen. Daher gibt es immer einen Kompromiss zwischen dem Sicherheitsniveau und seinen wirtschaftlichen Kosten und Vorteilen. Mit anderen Worten: Der Aufwand für einen Angriff muss in einem angemessenen Verhältnis zum Gewinn stehen, den Angreifende erzielen könnten. Die nachstehende Abbildung veranschaulicht eine mögliche Klassifizierung von Sicherheitsangriffen und -maßnahmen nach Kosten und Aufwand **Ungültige Quelle angegeben.**.

Kosten/Aufwand von Angriff versus Sicherheit

Grafik wird gelöscht

Quelle: Reza Vahidnia (2022)

IoT-Fachleuten stehen zahlreiche Maßnahmen zur Verfügung, mit denen sie die Sicherheitsherausforderungen bewältigen und die IoT-Geräte vor Angreifenden schützen können. Im Folgenden sind einige der wichtigsten Sicherheitstechniken aufgeführt, die von IoT-Entwickelnden berücksichtigt werden sollten (IoT Devices Security, 2017).

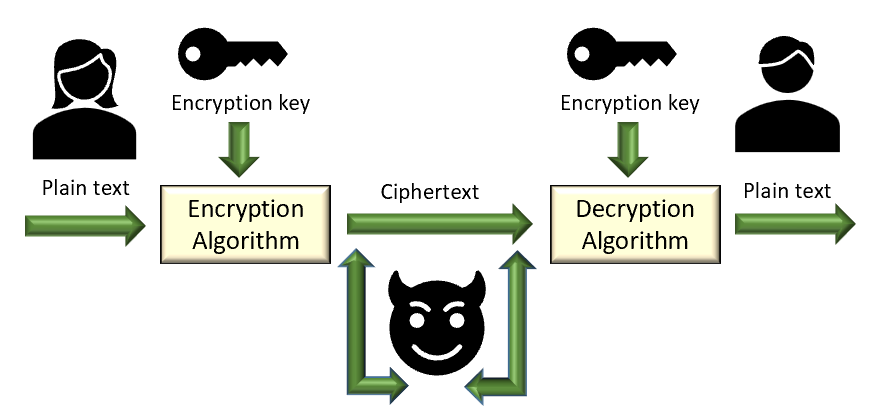
### Allgemeine Sicherheitstechniken

#### Paketverschlüsselung

Die Paketverschlüsselung, bei der die IoT-Klartextdaten in Chiffretext umgewandelt werden, ist das wichtigste Instrument zum Schutz der Datenvertraulichkeit vor unbefugtem Zugriff oder böswilliger Veränderung während der Übertragung zwischen IoT-Geräten und der Cloud. Die Ver- und Entschlüsselungsprozesse werden auf IoT-Geräten mit Hilfe von als Chiffre bezeichneten Algorithmen durchgeführt, die eine Reihe von Zahlen (Schlüssel) zur Ver- und Entschlüsselung der Daten verwenden. Bei symmetrischen Chiffren verwenden sowohl der Verschlüsselungs- als auch der Entschlüsselungsalgorithmus denselben Schlüssel. Asymmetrische Chiffren hingegen verwenden einen öffentlichen Schlüssel zur Verschlüsselung und einen privaten Schlüssel zur Entschlüsselung.

Bei den Verschlüsselungsalgorithmen kann es sich um einfache zeichenbasierte Chiffren handeln, bei denen jedes Zeichen im Klartext in ein anderes Zeichen im Chiffretext umgewandelt wird, oder um fortgeschrittene Algorithmen wie Data Encryption Standard (DES), Triple DES und Advanced Encryption Standard (AES), bei denen mehrere komplexe Durchgänge zur Verschlüsselung der Nachrichten durchgeführt werden.

Kryptografie



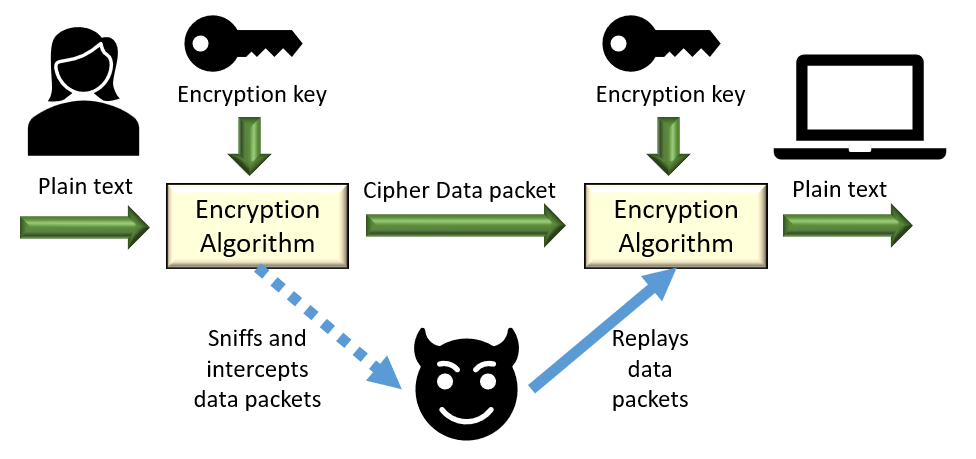
Quelle: Reza Vahidnia (2022) basierend auf encryption-and-authentication-in-the-iot (2022)

#### Schutz vor Nachrichtenwiederholung

Angreifende können verschlüsselte Nachrichten (Chiffretext), die zur Änderung des Zustands eines Aktors verwendet werden, aufzeichnen und später erneut senden und die ursprüngliche Aktion jederzeit wieder durchführen. So kann beispielsweise die verschlüsselte „Öffnen“-Nachricht, die von einem Smartphone gesendet wurde, von Angreifenden erneut gesendet werden, um das intelligente Schloss zu entsperren.

Der Zweck des Schutzes vor Nachrichtenwiederholung besteht darin, den Empfang aufgezeichneter doppelter Nachrichten zu vermeiden. Bei dieser Schutzmethode werden die verschlüsselten Pakete um Datenfelder (z. B. Datumsstempel) erweitert, die sich nach einem den Empfänger:innen bekannten Muster ändern. Die Empfänger:innen nehmen Nachrichten nur einmal und in einer bestimmten Reihenfolge an.

Nachrichtenwiederholung

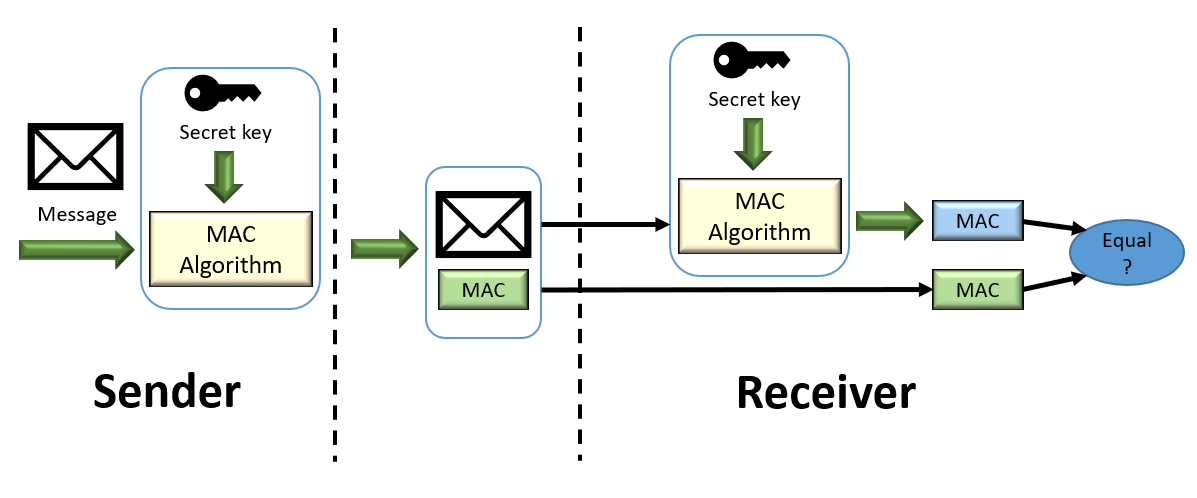


Quelle: Reza Vahidnia (2022)

#### Authentifizierungscode für Nachrichten

Bei diesem Verfahren mit geringer Komplexität wird eine kurze Signatur erstellt, indem ein Chiffrier- oder Hash-Algorithmus (eine Funktion, die eine Datenfolge in eine numerische Folge mit fester Länge umwandelt) auf ein Datenpaket angewendet wird. Diese Signatur begleitet das Datenpaket und wird von den Empfänger:innen mit demselben Chiffrier- oder Hash-Algorithmus verwendet, um zu gewährleisten, dass die Daten nicht verändert worden sind.

Authentifizierungscode für Nachrichten



Quelle: Reza Vahidnia (2022)

Die Nachrichtenauthentifizierung schützt IoT-Geräte vor Manipulationen und bietet einen sicheren Kanal für einige IoT-Geräte mit nicht vertraulichen Daten (z. B. Temperatursensoren), die ihre Daten im Klartext senden.

#### Schutz der Debug-Ports

Hardware-Ports wie JTAG und I2C, die für die Konfiguration, das Debuggen der Firmware und die Kommunikation mit anderen Geräten verwendet werden, sind verlockende Ziele für Hacker:innen. Hersteller von IoT-Geräten können diese Ports schützen, indem sie für jedes Gerät ein eindeutiges Passwort festlegen und die Ports in IoT-Geräten, die im Feld eingesetzt werden sollen, intern deaktivieren.

#### Sichere Bootloader (Startprogramme)

Die Hersteller von IoT-Geräten sollten die Geräte so konfigurieren, dass sie das Firmware-Image beim Starten überprüfen, um sicherzustellen, dass auf dem Gerät eine autorisierte Firmware läuft. Um die Firmware besser zu schützen, kann ihr Image auch verschlüsselt werden. Angreifende können außerdem Software-IPs ändern, deren Integrität nicht geschützt ist. Ein wirksamer Schutz gegen solche Änderungen ist die Versiegelung der Software-IP mit einer digitalen Signatur (Spitz, 2020).

#### Vorab mitgeteilte Schlüssel

Um die verschlüsselte Datenkommunikation zwischen IoT-Geräten besser zu schützen, werden die Verschlüsselungscodes vor der Datenübertragung zwischen IoT-Geräten über einen unabhängigen sicheren Kanal übermittelt und dann manuell auf die IoT-Geräte angewendet.

#### Secure Shell

Secure Shell (SSH) ist ein Protokoll zum Schutz von Debugging- und Konfigurationsports durch Verschlüsselung von Konsolenverbindungen, wie z. B. dem Linux-Shell-Zugang, was eine unbefugte Anzeige oder Bedienung verhindert.

#### Public-Key-Authentifizierung

In manchen Fällen ist es nicht sinnvoll, vorab mitgeteilte Schlüssel zu verwenden, weil der Schlüssel entweder nicht vom Hersteller konfiguriert werden kann, keine Expert:innen vor Ort verfügbar sind oder kein Schlüsselverteilungssystem existiert. In solchen Situationen wird Public Key Exchange (PKE, öffentlicher Schlüsselaustausch) verwendet, bei dem der öffentliche Schlüssel für jeden im Netz zugänglich ist. Das sendende IoT-Gerät verwendet den öffentlichen Schlüssel des empfangenden IoT-Geräts, um die Daten zu verschlüsseln, und das empfangende Gerät entschlüsselt die Nachricht dann mit seinem eigenen privaten Schlüssel.

Die Verwendung von PKE minimiert den manuellen Konfigurationsaufwand für die Einrichtung von IoT-Netzwerken, da Sender und Empfänger ihre Schlüssel nicht kennen müssen, bevor sie eine Verbindung herstellen. PKE wird normalerweise bei Linux-basierten Systemen verwendet, wo die erforderlichen Ressourcen bereits vorhanden sind.

#### Transport Layer Security

Transport Layer Security (TLS, Transportschichtsicherheit) ist ein auf größeren und leistungsfähigeren IoT-Geräten verwendeter Standard, der das Transmission Control Protocol (TCP) unterstützt und den Datenaustausch im Netzwerk durch die Bereitstellung eines Standardrahmens für PKE und Verschlüsselung sichert.

#### Wi-Fi Protected Access 2 (WPA2)

WPA2 ist eine Reihe von weit verbreiteten Sicherheitsstandards, die von der Wi-Fi Alliance entwickelt wurden und zur Sicherung des Wi-Fi-Kommunikationskanals in größeren und leistungsfähigeren IoT-Geräten verwendet werden. Im Vergleich zu Wired Equivalent Privacy (WEP), dem ursprünglichen Wi-Fi-Sicherheitsstandard, bietet WPA2 eine ausgefeiltere Datenverschlüsselung und eine verbesserte Authentifizierung der Benutzenden.

### Fragen zur Selbstkontrolle

1. Erläutern Sie bitte, wie ein Nachrichtenauthentifizierungscode zur Erhöhung der Sicherheit von IoT-Geräten beitragen kann.

Es wird eine kurze Signatur erstellt, indem ein Chiffrier- oder Hash-Algorithmus auf ein Datenpaket angewendet wird. Diese Signatur begleitet das Datenpaket und wird von den Empfänger:innen mit demselben Chiffrier- oder Hash-Algorithmus verwendet, um zu gewährleisten, dass die Daten nicht verändert worden sind.

1. Bitte erläutern Sie, wie ein sicherer Bootloader zur Sicherung von IoT-Geräten eingesetzt wird.

Die Hersteller von IoT-Geräten sollten die Geräte so konfigurieren, dass sie das Firmware-Image beim Starten überprüfen, um sicherzustellen, dass auf dem Gerät eine autorisierte Firmware läuft. Um die Firmware besser zu schützen, kann ihr Image auch verschlüsselt werden.

Zusammenfassung

IoT-Geräte haben mehrere Angriffsebenen, darunter Hardware, Firmware, Betriebssystem, Anwendung, Web-Interface, Protokolle und Richtlinien. Jede Angriffsebene hat ihre eigenen Sicherheitsprobleme und damit verbundenen Risiken. Die Sicherheitsrisiken von IoT-Geräten werden klassifiziert nach dem, was sie bedrohen: Vertraulichkeit, Verfügbarkeit, Datenintegrität und den Diebstahl von Diensten. Die Sicherheitstechniken und -mechanismen, die für PCs und Smartphones verwendet werden, lassen sich aufgrund der begrenzten Ressourcen und der einfachen Schnittstellen nicht ohne weiteres auf IoT-Geräte übertragen.

IoT-Fachleuten stehen zahlreiche Maßnahmen zur Verfügung, mit denen sie die Sicherheitsherausforderungen bewältigen und die IoT-Geräte vor Angreifenden schützen können. Paketverschlüsselung, Schutz vor Nachrichtenwiederholung, Authentifizierungscodes für Nachrichten, Schutz der Debug-Ports, Sichere Bootloader, vorab mitgeteilte Schlüssel, Secure Shell, Public-Key-Authentifizierung, TLS und WPA2 sind einige der wichtigsten Techniken, die zum Schutz von IoT-Geräten vor Sicherheitsangriffen eingesetzt werden.

# Lektion 5 – Operative Sicherheit

**Lernziele**

Nach dem Abschluss dieser Lektion werden Sie...

... die Funktion und den Nutzen von Informations- und Cybersicherheitsmanagementsystemen erläutern können.

... die Netzwerksicherheitslösungen identifizieren können.

... die Best Practices für die Gerätekonfiguration auflisten können, mit denen IoT-Systeme gesichert werden.

... den Authentifizierungsprozess beim TSL-Handshake beschreiben können.

# 5. Operative Sicherheit

## Einführung

Operative Sicherheit (OPSEC, operational security) oder prozedurale Sicherheit zielt auf den Schutz sensibler Daten ab, indem die Systemoperationen aus der Sicht der Angreifenden betrachtet und getestet werden. Im Folgenden sind die fünf Schritte und Elemente aufgelistet, die in OPSEC verwendet werden und Führungskräfte dazu ermutigen, ihre Operationen zu überprüfen und herauszufinden, wo ihre Daten potenziell beeinträchtigt werden könnten:

* Identifizierung sensibler Daten, die geschützt werden müssen.
* Identifizierung möglicher interner und externer Bedrohungen für jede Kategorie sensibler Daten (Sicherheitsüberwachung).
* Bewertung von Sicherheitslücken und Schwachstellen, die zum Zugriff auf sensible Daten ausgenutzt werden könnten.
* Bewertung des Risikos und Einstufung der Schwachstellen basierend auf der Wahrscheinlichkeit eines Angriffs sowie des Aufwands und der Zeit, die zur Wiederherstellung erforderlich wären.
* Erstellung und Umsetzung eines Plans zur Risikominderung und Bedrohungsbeseitigung.

Mit Hilfe der oben genannten fünf Schritte können Führungskräfte Schwachstellen aufdecken und die richtigen Gegenmaßnahmen zum Schutz sensibler Informationen ergreifen. Zur Implementierung eines robusten und umfassenden OPSEC-Systems sollten alle Netzwerkänderungen protokolliert und kontrolliert, der Zugang zu Netzwerkgeräten auf autorisierte Benutzende beschränkt (Prinzip des geringsten Privilegs), und menschliche Eingriffe durch Aufgabenautomatisierung reduziert werden.

## 5.1 Informations- und Cybersicherheitsmanagementsystem

Ein Informations- und Cybersicherheitsmanagementsystem (ICSMS) dient dem Schutz der Vertraulichkeit, Integrität und Verfügbarkeit der Daten eines Unternehmens oder einer Organisation vor potenziellen Sicherheitsbedrohungen.

* Die Datenvertraulichkeit wird dadurch gewahrt, dass der Datenzugang nur für autorisierte Benutzende möglich ist. Jeder Verstoß gegen den Datenschutz ist eine Verletzung der Vertraulichkeit.
* Die Datenintegrität wird geschützt, indem die Datenkorrektheit und -vollständigkeit sichergestellt sind. Eine Verletzung der Datenintegrität durch Angreifende beeinträchtigt sensible Informationen.
* Datenverfügbarkeit bedeutet, dass die Informationen für autorisierte Benutzende verfügbar sein müssen. Die Datenverfügbarkeit kann durch [Verteilte-Denial-of-Service-Angriffe](https://www.checkpoint.com/cyber-hub/cyber-security/what-is-ddos/) (DDoS) gefährdet sein.

Das ICSMS identifiziert die potenziellen Risiken für eine Organisation und bewertet deren Wahrscheinlichkeit und mögliche Auswirkungen. Es entwickelt und implementiert auch Lösungsstrategien, um das Risiko unter Einsatz der verfügbaren Ressourcen zu mindern.

### ICSMS-Normen und -Anwendung

Das ICSMS-Programm einer Organisation kann durch verschiedene Faktoren bestimmt werden, darunter interne Richtlinien der Organisation oder externe Datenschutzvorschriften. Für jeden dieser internen und externen Faktoren gibt es eigene Normen und deren Anwendungen, wie z. B. die ISO 27001, eine internationale Norm, die bewährte Sicherheitspraktiken beschreibt und die Einführung eines Managementsystems für Informationssicherheit vorschreibt. Wenn eine Organisation nach ISO 27001 zertifiziert werden will, muss sie deren Anforderungen umsetzen.

Einige Beispiele für externe Datenschutzbestimmungen sind die folgenden (What is information security management, 2022):

* [Payment Card Industry Data Security Standard (PCI DSS)](https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cspm-cloud-security-posture-management/pci-dss-compliance/) ist eine vom Finanzsektor entwickelte Norm, die auf den Schutz aller an einer Kartentransaktion beteiligten Daten abzielt (z. B. den Transaktionswert). Zu beachten ist, dass sich PCI DSS nicht auf den Datenschutz, sondern auf die Sicherheit von Kartenzahlungen bezieht.
* [General Data Protection Regulation (GDPR)](https://www.checkpoint.com/solutions/gdpr/) ist eine allgemeine Datenschutzverordnung, welche die persönlich identifizierbaren Informationen (PII) der Bürger:innen der Europäischen Union durch strenge Anforderungen an den Schutz der Privatsphäre und an die Datensicherheit schützen soll.
* [Health Insurance Portability and Accessibility Act (HIPAA) ist eine US-Verordnung für das Gesundheitswesen, die Sicherheitskontrollen für geschützte Gesundheitsinformationen vorschreibt.](https://www.checkpoint.com/cyber-hub/cyber-security/what-is-hipaa-compliance/)

Die vorgenannten Datenschutzbestimmungen verlangen explizit oder implizit, dass das Managementprogramm für Informationssicherheit umgesetzt wird. Die Einführung eines ICSMS schafft einen Bewertungsrahmen für Datensicherheitsrisiken und Verfahren zu deren Minderung. Außerdem macht es die Datensicherheit effizienter, indem es die Sicherheitsarchitektur des Unternehmens optimiert und unnötige Maßnahmen unterlässt. Ein ICSMS kann auch den Ruf einer Organisation und ihre Beziehungen zu Partnern und Kund:innen verbessern.

### Fragen zur Selbstkontrolle

1. Erläutern Sie bitte die Vorteile der Einführung eines ICSMS für Unternehmen.

Die Einführung eines ICSMS schafft einen Bewertungsrahmen für Datensicherheitsrisiken und Verfahren zu deren Minderung. Außerdem macht es die Datensicherheit effizienter, indem es die Sicherheitsarchitektur des Unternehmens optimiert und unnötige Maßnahmen unterlässt. Ein ICSMS kann auch den Ruf einer Organisation und ihre Beziehungen zu Partnern und Kund:innen verbessern.

1. Bitte wählen Sie den Begriff aus, der den Datenschutz durch Zugriffsbeschränkung auf autorisierte Benutzende bezeichnet.

* Datenintegrität
* Datenvertraulichkeit
* Datenverfügbarkeit
* Datenkonformität

## 5.2 Netzwerksicherheit

Die von IoT-Sensoren gesammelten Daten müssen auf dem Weg zur Cloud-Anwendung vor Cyberangriffen geschützt werden. Ein gut gesichertes Netzwerk schützt Unternehmen und Einzelpersonen und verhindert Datenverluste und Datenschutzverletzungen. Es gibt viele Lösungen für die Netzwerksicherheit, die gewährleisten, dass Daten nicht angegriffen oder von unautorisierten Benutzenden angesehen werden. Einige dieser Lösungen werden im Folgenden näher erläutert.

### Firewall

**Virtual Private Network**

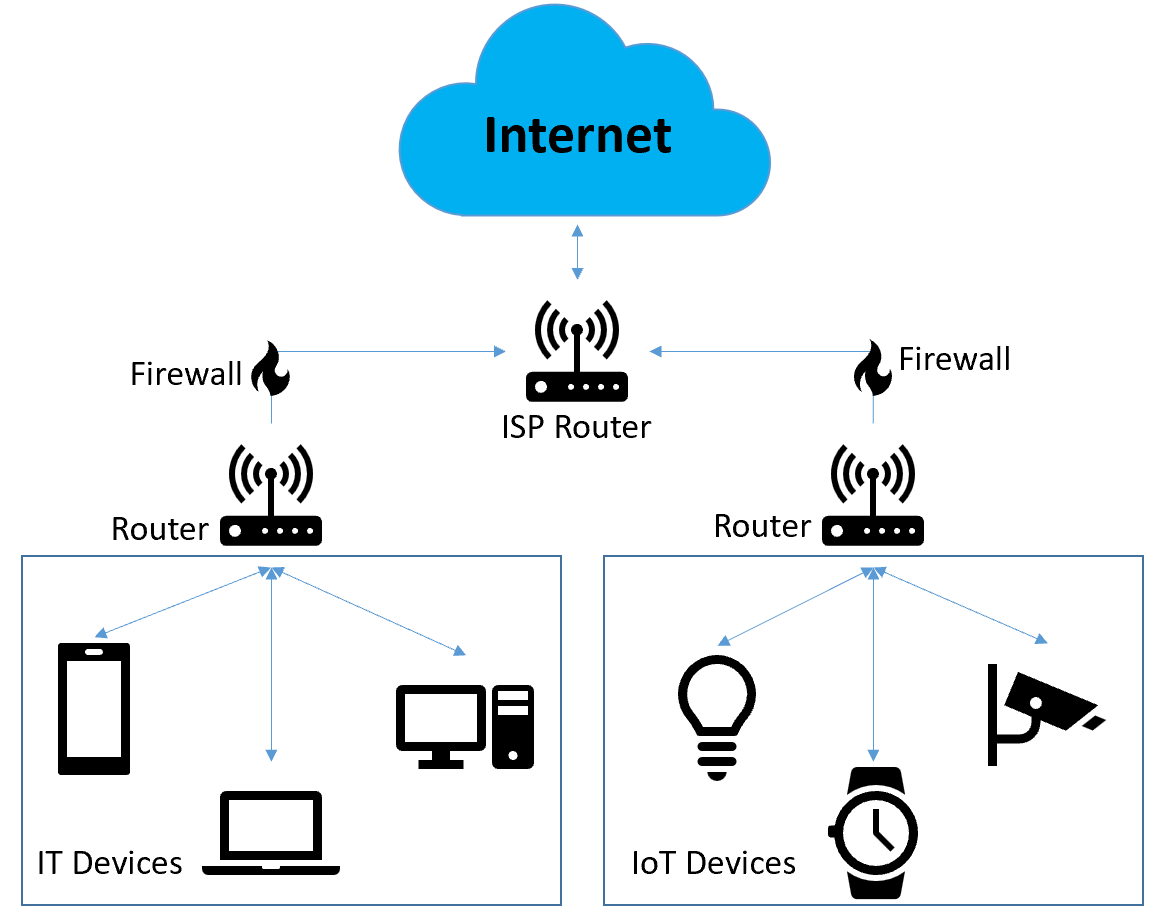
Private Netzwerkverbindung, die zum Schutz von Daten in öffentlichen Netzwerken verwendet wird.

Firewalls definieren Sicherheitsregeln zur Kontrolle der aus- und eingehenden Netzwerkdaten. Firewalls können Malware und Sicherheitsangriffe auf der Anwendungsebene abwehren. IoT-Systeme profitieren von Firewalls, mit denen ihre Geräte vor Angriffen geschützt werden. Es gibt zwei Varianten für die Implementierung von IoT-Firewalls. Eine Netzwerk-Firewall kann als Teil der Netzwerk-Gateways eingesetzt werden, indem ein **Virtual Private Network** (VPN, virtuelles privates Netzwerk) zur Verschlüsselung der Daten zwischen den IoT-Gateways und dem Server verwendet wird. Dieser Ansatz eignet sich für einfache IoT-Geräte ohne integrierte Firewalls. Alternativ können IoT-Firewalls in das Betriebssystem der IoT-Geräte eingebettet werden, die somit durch die Filterung der Daten als VPN-Endpunkt fungieren.

### Netzwerksegmentierung

Bei der Netzwerksegmentierung wird ein größeres Netzwerk in mehrere logische oder physische Teilnetze unterteilt, die auf den gemeinsamen Funktionen und Rollen der Geräte und Komponenten basieren. Die Netzwerksegmentierung kann die Leistung und Sicherheit des Netzwerks erhöhen. Dieser Ansatz ist besonders wichtig für die Trennung von IT- und IoT-Systemen, um zu verhindern, dass kompromittierte Geräte das gesamte System infizieren. Durch die Netzwerksegmentierung können IoT-Geräte nicht miteinander kommunizieren, so dass die IoT-Daten und die Kommunikation mit den Diensten besser kontrolliert und verwaltet werden können **Ungültige Quelle angegeben.**.

Netzwerksegmentierung



Quelle: Reza Vahidnia (2023), basierend auf home-network-segmentation-a-must-in-the-iot-er (2018)

Ein neuerer Ansatz zur Sicherung des Netzwerks ist die Mikrosegmentierung, bei der das Datenzentrum logisch in mehrere Sicherheitssegmente aufgeteilt wird. Anschließend werden für jedes Segment eigene Sicherheitsrichtlinien definiert, damit Sicherheitsarchitekt:innen flexible Sicherheitskontrollen einsetzen können, ohne mehrere Firewalls installieren zu müssen (micro-segmentation, 2023).

### Zugriffskontrolle

Richtlinien für die Zugriffskontrolle können den unbefugten Zugriff auf Anwendungen verhindern, indem sie festlegen, welche Benutzenden und Geräte auf der Grundlage ihrer Rollen Zugriff auf welche Ressourcen und Daten haben.

### Remote Access VPN

Remote Access VPN ermöglicht Geräten und Benutzenden von überall den sicheren Zugriff auf das private Netzwerk eines Unternehmens, indem ein privater Tunnel zwischen dem Gerät/den Benutzenden und dem privaten Netzwerk des Unternehmens aufgebaut und die Daten Ende-zu-Ende verschlüsselt werden. Obwohl Remote Access VPN für Organisationen große Vorteile hat, können damit einige Risiken und Schwachstellen verbunden sein. Dazu gehören (remote-access-vpn, 2023):

* Benutzende mit zu vielen Berechtigungen, die auf nicht zugelassene Ressourcen im Netzwerk zugreifen können.
* unsichere Endpunkte, die Malware in das Netzwerk einschleusen können.
* auswärtige Benutzende ohne Zugriff auf den gesamten Sicherheitsumfang.
* einzelner Schwachpunkt, der zu einer Betriebsunterbrechung führen kann.
* Ein Hack des VPN kann die gesamte Organisation gefährden.
* Böswillige Benutzende können aus der Ferne einen Insider-Angriff durchführen, ohne dass Netzwerkadministrierende Einblick in die Vorgänge innerhalb der VPN-Verbindung haben.

### Zero Trust Network Access (ZTNA)

ZTNA (Null-Vertrauen-Netzwerkzugang), auch Software defined Perimeter (SDP) genannt, ermöglicht es den Benutzenden, nur auf die Ressourcen zuzugreifen, die sie zur Erfüllung ihrer Aufgaben benötigen (im Gegensatz zu VPN, das Zugang zum gesamten Netz gewährt). Sobald eine Person authentifiziert ist, stellt ZTNA ihr einen sicheren und verschlüsselten Tunnel zur Verfügung, so dass sie keinen Einblick in andere Anwendungen oder Dienste hat, auf die sie nicht zugreifen darf. ZTNA kann auch Sicherheitskontrollen basierend auf dem Standort oder den Spezifikationen des Geräts einrichten, um zu verhindern, dass kompromittierte Geräte auf die Netzwerkressourcen zugreifen.

### Data Loss Prevention (DLP)

DLP-Software (Software zur Verhinderung von Datenverlusten) zielt darauf ab, unbefugten Zugriff zu verhindern, indem sie potenzielle Datenschutzverletzungen erkennt und die sensiblen Daten während der Nutzung, bei der Übertragung und im Ruhezustand kontinuierlich überwacht.

### Intrusion-Prevention-Systeme (IPS)

IPS-Technologien (Systeme zur Verhinderung von Intrusionen) erkennen böswillige Aktivitäten, die versuchen, eine Schwachstelle auszunutzen, und blockieren Angriffe auf die Netzwerksicherheit wie Denial-of-Service (DoS) oder **Brute-Force-Angriffe**.

**Brute-Force-Angriff**

Erraten des Passworts durch Eingabe zu vieler möglicher Varianten.

### Sandboxing

Beim Sandboxing werden Codes und Dateien in einer isolierten und sicheren Umgebung ausgeführt und getestet, in der die Betriebsumgebungen der Endbenutzenden nachgeahmt werden. Somit wird verhindert, dass sich Sicherheitsbedrohungen auf das gesamte Netzwerk ausbreiten.

### Hyperscale-Netzwerk-Sicherheit

Hyperscale-Netzwerk-Sicherheit sorgt für eine nahtlose Erweiterung der Netzwerksicherheitsarchitektur, indem sie mehrere Maßnahmen durchführt. Zum Beispiel behandelt sie eine Anordnung von Firewalls als eine einzige Einheit und ermöglicht lokalen Systemen ein ähnliches Niveau an Ausfallsicherheit zu erreichen wie die öffentliche Cloud, jedoch ohne deren Sicherheitsprobleme.

### Fragen zur Selbstkontrolle

1. Bitte erläutern Sie, wie Netzwerksegmentierung die Netzwerksicherheit erhöhen kann.

Bei der Netzwerksegmentierung wird ein größeres Netzwerk in mehrere logische oder physische Teilnetze unterteilt, die auf den gemeinsamen Funktionen und Rollen der Geräte und Anlagen basieren und verhindern, dass kompromittierte Geräte das gesamte System infizieren.

1. Bitte wählen Sie aus, welche Netzwerksicherheitslösung Sicherheitsregeln zur Kontrolle der aus- und eingehenden Netzwerkdaten definiert.

* Data Loss Prevention
* Intrusion-Prevention-Systeme
* Hyperscale-Netzwerk-Sicherheit
* Firewall

## 5.3 Gerätekonfiguration

Das IoT-Gerätemanagement sollte bewährte Verfahren und Richtlinien befolgen, damit die Geräte so konfiguriert sind, dass Sicherheitsbedrohungen minimiert werden. Im Folgenden finden Sie einige bewährte Verfahren für die Gerätekonfiguration, die eine Beeinträchtigung von IoT-Geräten verhindern (iotdevices, 2023).

### Zugriff

IoT-Geräte sollten so konfiguriert werden, dass sie jeden unbefugten Zugriff unterbinden. Häufiges Ändern der Passwörter und die Wahl komplexer Passwörter ist eine der Optionen. Außerdem sollte sichergestellt werden, dass kein unverschlüsselter Kanal wie HTTP Zugang zur Verwaltungsschnittstelle des IoT-Geräts hat. Statt HTTP sollte HTTPS für den Zugriff auf die Verwaltungsschnittstellen verwendet werden.

Alle unnötigen Dienste auf den Geräten sollten deaktiviert werden. Bei IoT-Geräten, die einen Raspberry Pi als Rechenmodul verwenden, sollte die SSHD-Konfiguration so geändert werden, dass nur bestimmte Benutzende Zugang zu SSH haben. Außerdem wird empfohlen, am Gerät eine schlüsselbasierte Authentifizierung anstelle einer Anmeldung mit Benutzernamen und Passwort zu verwenden.

### Software-Updates

Die Firmware der IoT-Geräte sollte mit den neuesten Versionen und Sicherheitspatches aktualisiert werden, die der Hersteller bereitstellt. Beachten Sie, dass manchmal Sicherheits-Patches zu einer Änderung des Passworts führen können.

### Dienste

Alle unnötigen Dienste, wie E-Mail, FTP, SSH, Multicast Ipv4 und Telnet sollten auf den Geräten deaktiviert werden. Sobald Daten von der Cloud-Anwendung empfangen und bestätigt wurden, können sie auf dem IoT-Gerät gelöscht werden. Die Löschung sollte bestätigt werden, damit keine Daten auf dem Gerät verbleiben.

### Netzwerk

Wenn möglich, sollten IoT-Geräte eine nicht öffentlich routingfähige IP-Adresse verwenden. Außerdem sollten nur bestimmte IP-Adressen auf das IoT-Gerätemanagement zugreifen können. Alle anderen IP-Adressen sollten mit Hilfe einer Firewall geblockt und eingeschränkt werden.

### Protokollierung

Zugriffe auf die IoT-Geräte und Konfigurationsänderungen sollten protokolliert und überwacht werden, um ungewöhnliches Verhalten zu erkennen.

### Redundanz und Backups

Von der Konfiguration der IoT-Geräte sollten regelmäßig Backups erstellt werden. Zu diesem Zweck kann ein externes System verwendet werden, um die Konfigurationsänderungen zu verfolgen.

### Fragen zur Selbstkontrolle

1. Noch zu ergänzen

## 5.4 Authentifizierung and Autorisierung

**Transport Layer Security (TLS)**

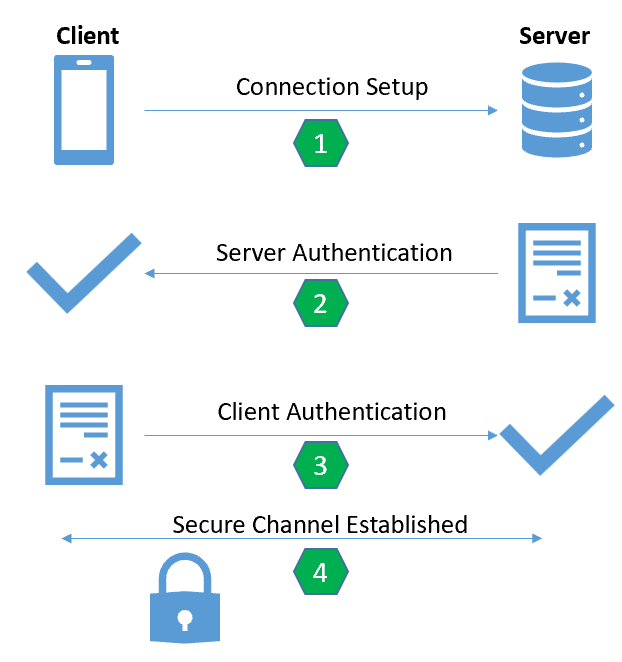
Ein weit verbreitetes kryptografisches Protokoll für die sichere Kommunikation in Computernetzen.

Autorisierung oder Zugriffskontrolle bezieht sich auf den Prozess der Bestimmung, ob Benutzenden oder Geräten der Zugriff auf die Ressourcen erlaubt, verweigert oder entzogen wird. Damit Geräte oder Benutzende für den Zugriff auf Ressourcen autorisiert werden können, müssen sie zunächst ordnungsgemäß authentifiziert oder gegenüber dem System identifiziert werden. Wenn das IoT-Gerät und der Server nicht ordnungsgemäß identifiziert werden, sind die Daten nicht vertrauenswürdig.

In einem Client-Server-Kommunikationsschema wird ein kryptografisches Handshake-Protokoll wie **Transport Layer Security (TLS)** verwendet, um eine Verbindung zwischen dem IoT-Gerät und dem Server zu authentifizieren.

Die nachstehende Abbildung veranschaulicht die erforderlichen Schritte für die Authentifizierung im TLS-Handshake-Verfahren.

Mutual Client-Server Authentication in TLS-Handshake

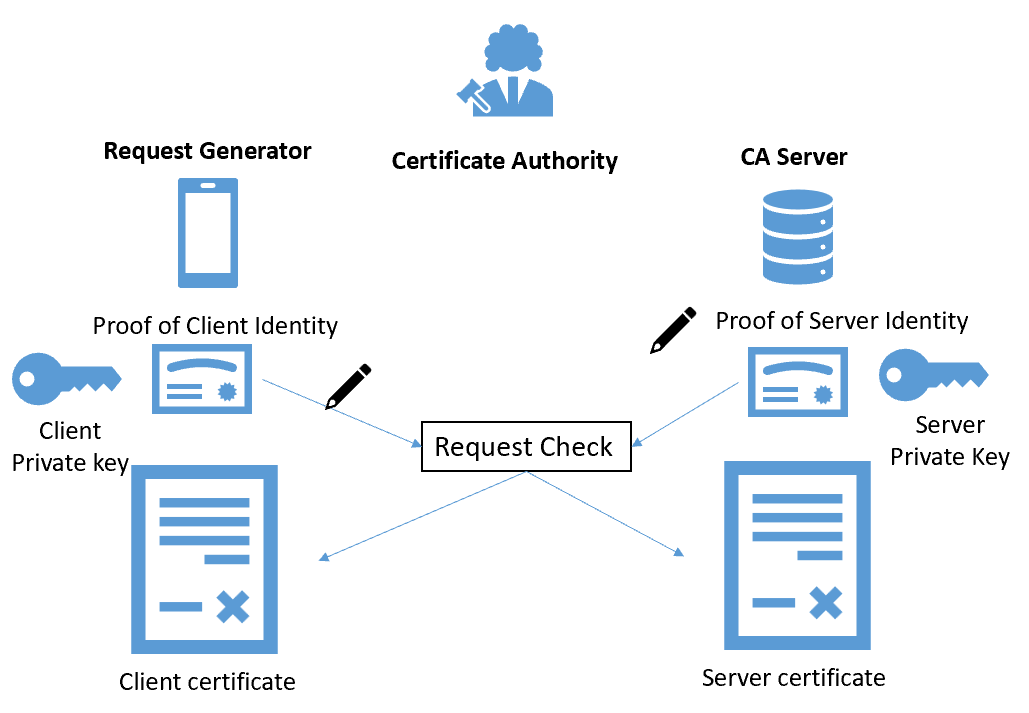


Quelle: Reza Vahidnia (2023), basierend auf Grover (2022)

In Schritt 1 stellt das IoT-Gerät (Client) eine Verbindung zum Server her. In Schritt 2 präsentiert der Server dem Client seine Identität durch Vorlage eines Zertifikates, das von einer Zertifizierungsstelle (CA) unterzeichnet wurde, welcher der Client vertraut. Diese ist dafür verantwortlich, die Identität des Servers zu bestätigen und zu validieren. In Schritt 3 verwendet das IoT-Gerät sein CA-Zertifikat, um dem Server mitzuteilen, dass es ein gültiges und legitimes Zertifikat besitzt. Es ist zu beachten, dass die Sicherheit der Zertifizierungsstelle im TLS-Protokoll von entscheidender Bedeutung ist. Wenn sie kompromittiert wird, kann die gesamte Kommunikation gehackt werden. Schließlich wird in Schritt 4 ein gesicherter verschlüsselter Kanal zwischen dem Client und dem Server für die vertrauliche Kommunikation eingerichtet.

Die folgende Abbildung zeigt, wie der Client und der Server Zertifikate von der Zertifizierungsstelle anfordern.

Requesting Certificates From a CA



Quelle: Reza Vahidnia (2023), basierend auf Grover (2022)

Im Prinzip ist eine Zertifizierungsstelle die Einheit, die einem IoT-Gerät eine eindeutige Identität in Form eines digitalen Zertifikats zuweist. Dieser Prozess findet in der Regel in einer sicheren Umgebung während der Herstellung statt und wird als Provisioning bezeichnet. Er ist ein fester Bestandteil der Lieferkettensicherheit von IoT-Geräten. Wenn der CA-Schlüssel offengelegt wird, kann jeder, der ihn hat, auf die Geräte zugreifen. Aus diesem Grund muss der Provisioning-Prozess geheim gehalten werden, und deshalb bieten die Zertifizierungsstellen IoT-Gerätezertifikate als Dienstleistung für Erstausrüster (OEMs) an. Bei diesem Modell vergeben die Erstausrüster die sichere Verwaltung ihrer CA-Schlüssel an eine dritte Partei, die sich um die Aufhebung und Erneuerung von Zertifikaten kümmert (IoTSF, 2021)**.**

Der Provisioning-Prozess kann auf zwei Arten erfolgen. Beim ersten Ansatz wird eine einmalige Seriennummer entnommen und in einer Datenbank auf dem Server gespeichert, um das IoT-Gerät zu verifizieren. Bei der zweiten Methode, die einfacher für die Gerätehersteller ist, wird bei der Fertigung oder später beim Einsatz durch vertrauenswürdige Benutzende ein unterzeichnetes Zertifikat (Authentifizierungs-ID) in das Gerät eingebracht. Beim zweiten Ansatz fehlt jedoch die Identitätsverfolgung für die ausgelieferten Geräte, und die Kontrolle der Kundengeräte nach ihrer Bereitstellung wird erschwert. Der andere Nachteil der zweiten Methode ist, dass der Server die IoT-Geräte ungeachtet ihrer Besitzenden behandelt. Das bedeutet, dass ein unfreiwilliger Besitzerwechsel, wie z. B. durch Diebstahl, dazu führen kann, dass sich ein nicht mehr vertrauenswürdiges Gerät im Netz befindet.

### Fragen zur Selbstkontrolle

1. Bitte erläutern Sie die beiden Arten des Bereitstellungsprozesses für IoT-Geräte.

Beim ersten Ansatz wird eine einmalige Seriennummer entnommen und in einer Datenbank auf dem Server gespeichert, um das IoT-Gerät zu verifizieren. Bei der zweiten Methode wird bei der Fertigung oder später beim Einsatz durch vertrauenswürdige Benutzende ein unterzeichnetes Zertifikat (Authentifizierungs-ID) in das Gerät eingebracht.

1. Bitte erläutern Sie, was mit Provisioning für ein IoT-Gerät gemeint ist.

Der Prozess, bei dem IoT-Geräte während der Herstellung eine eindeutige Identifizierung erhalten, wird als Provisioning bezeichnet.

Zusammenfassung

Das Hauptziel eines Informations- und Cybersicherheitsmanagementsystems (ICSMS) besteht darin, die Vertraulichkeit, Integrität und Verfügbarkeit der Unternehmensdaten vor potenziellen Sicherheitsbedrohungen zu schützen. Außerdem müssen die von IoT-Sensoren gesammelten Daten auf dem Weg zur Cloud-Anwendung vor Cyberangriffen geschützt werden.

Es gibt viele Netzwerksicherheitslösungen, die gewährleisten, dass Daten nicht angegriffen oder von unautorisierten Benutzenden angesehen werden. Einige dieser Lösungen sind: Firewall, Netzwerksegmentierung, Zugriffskontrolle, Remote Access VPN, Zero Trust Network Access (ZTNA), Data Loss Prevention (DLP), Intrusion Prevention Systems (IPS), Sandboxing und Hyperscale-Netzwerk-Sicherheit.

Aus Geräteperspektive sollte das IoT-Gerätemanagement bewährte Verfahren und Richtlinien befolgen, damit die Geräte so konfiguriert sind, dass Sicherheitsbedrohungen minimiert werden. Andernfalls kann durch ein einziges kompromittiertes IoT-Gerät das gesamte IoT-System der Gefahr eines Angriffs durch böswillige Benutzende ausgesetzt werden.

Die Autorisierung oder Zugriffskontrolle bestimmt, ob Benutzenden oder Geräten der Zugriff auf die Ressourcen erlaubt, verweigert oder entzogen wird. Damit Geräte oder Benutzende für den Zugriff auf Ressourcen autorisiert werden können, müssen sie zunächst ordnungsgemäß authentifiziert oder gegenüber dem System identifiziert werden. Wenn das IoT-Gerät und der Server nicht ordnungsgemäß identifiziert werden, sind die Daten nicht vertrauenswürdig. In einem Client-Server-Kommunikationsschema wird ein kryptografisches Handshake-Protokoll wie Transport Layer Security (TLS) verwendet, um eine Verbindung zwischen dem IoT-Gerät und dem Server zu authentifizieren.

# Lektion 6 – Cloud-Sicherheit

**Lernziele**

Nach dem Abschluss dieser Lektion werden Sie...

... die drei verschiedenen Cloud-Service-Modelle beschreiben können.

... das Schichtenmodell des Fog Computings sowie seine Herausforderungen, Vorteile und Nachteile erläutern können.

... die kritischsten Cloud-basierten Sicherheitsbedrohungen auflisten und erläutern können.

... die gängigsten Cloud-basierten Sicherheitsdienste identifizieren können.

# 6. Cloud-Sicherheit

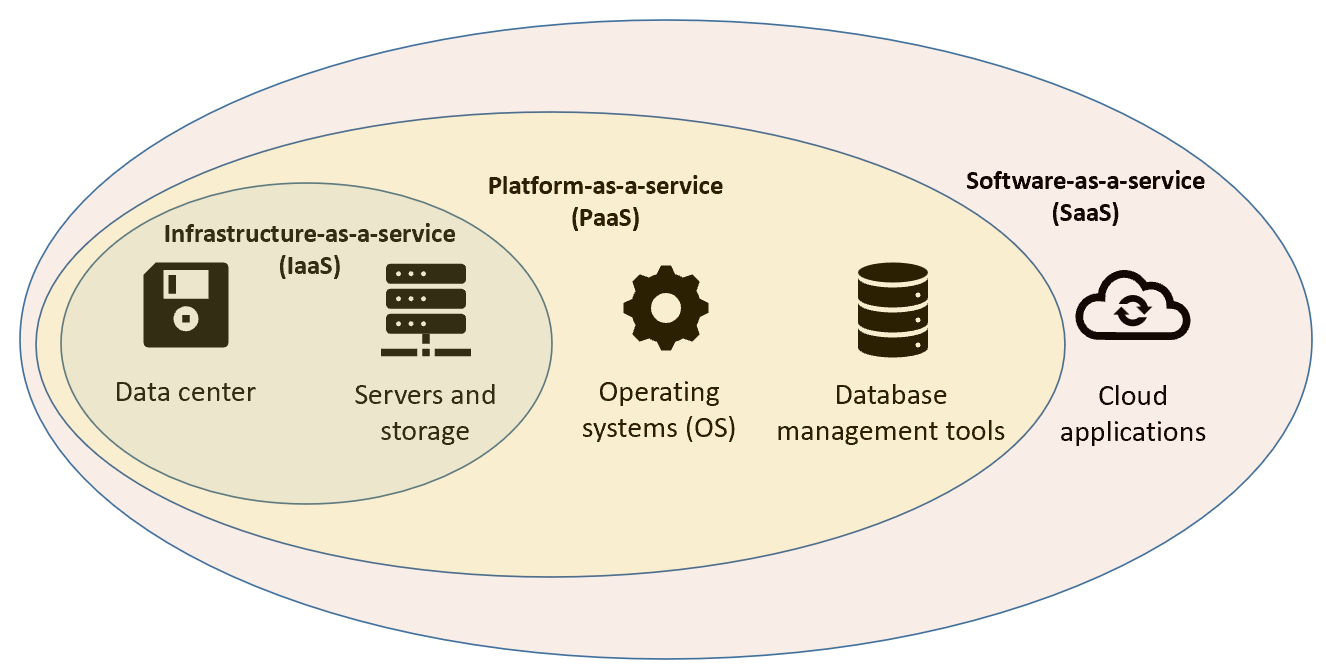
## Einführung

Eine Ansammlung von Servern, auf denen Datenbanken und Software laufen, wird als Cloud bezeichnet. Diese Server sind mit dem Internet verbunden und befinden sich in Datenzentren auf der ganzen Welt. Die Nutzung von Cloud-Diensten senkt einige IT-Kosten für Unternehmen und kleine Betriebe und ermöglicht es Unternehmen und Einzelpersonen, von jedem Gerät und von überall auf ihre Dateien zuzugreifen und ihre Anwendungen auf diesen Servern auszuführen, ohne sich um die Verwaltung ihrer eigenen physischen Server kümmern zu müssen.

Wie die folgende Abbildung zeigt, gibt es drei verschiedene Servicemodelle, die von Cloud-Service-Anbietern bereitgestellt werden (what-is-the-cloud, 2023). Zu diesen Modellen gehören:

* **Software as a Service (SaaS):** Bei diesem Modell hostet der Cloud-Service-Anbieter die Anwendungen auf der Cloud und ermöglicht den Nutzenden den Zugriff darauf. Daher müssen die Nutzenden die Anwendungen nicht auf ihren eigenen Geräten installieren. Salesforce ist ein Beispiel für SaaS.
* **Platform as a Service (PaaS):** Bei diesem Modell liefern die Anbieter die notwendigen Entwicklungswerkzeuge wie Infrastruktur und Betriebssysteme, damit die Benutzenden ihre Anwendungen erstellen können. Microsoft Azure ist ein Beispiel für PaaS.
* **Infrastructure as a Service (IaaS):** Bei diesem Modell mieten die Nutzenden die Server und den Speicher in der Cloud, um ihre Anwendungen mit ihren eigenen Entwicklungstools zu erstellen. Google Compute Engine und OpenStack sind zwei Beispiele für IaaS.

Cloud Service Models



Quelle: Reza Vahidnia (2023), basierend auf what-is-the-cloud (2023)

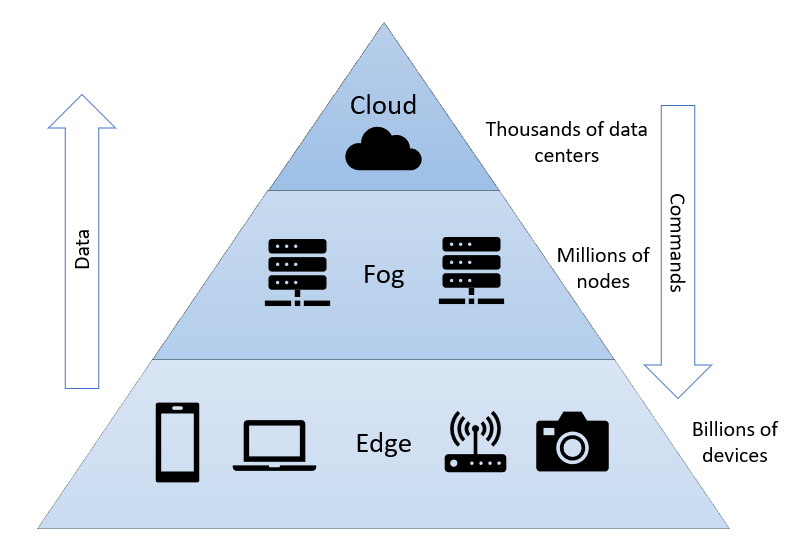
In der Welt des IoT kann die Cloud dabei helfen, die von verschiedenen Sensoren in unterschiedlichen geografischen Gebieten gesammelten Daten zu speichern und zu analysieren. Neben den großen Vorteilen kann jedoch jede Sicherheitsverletzung in der Cloud das gesamte IoT-Ökosystem gefährden, das die Cloud-Dienste nutzt, einschließlich der Geräte, Datenbanken und Anwendungen. Daher ist es äußerst wichtig, die Schwachstellen der Cloud zu verstehen und die notwendigen Sicherheitsmechanismen zum Schutz von IoT-Lösungen zu implementieren.

## 6.1 Konzept des Fog Computings

Bei IoT-Anwendungen ist es nicht immer notwendig oder möglich, alle Sensordaten zur weiteren Verarbeitung und Speicherung in die Cloud zu senden. Zeitkritische Anwendungen vertragen keine hohen Latenzzeiten für die Übertragung der Daten in die Cloud und das Warten auf eine Entscheidung oder einen Befehl aus der Cloud. Stattdessen werden in solchen Szenarien die Daten in den Ressourcen und in der Infrastruktur verarbeitet, die sich zwischen dem Datenendpunkt (d. h. dem IoT-Sensor) und der Cloud befinden. Diese dezentralisierte Form der Datenverarbeitung wird als Fog Computing bezeichnet, bei dem die Daten an Netzwerkknoten wie Switches und Routern verarbeitet werden.

Fog Computing spart Bandbreite, da nicht alle Rohdaten in die Cloud übertragen werden, und erhöht die Sicherheit und den Schutz sensibler Daten, die eine bestimmte Organisation oder einen bestimmten Standort nicht verlassen müssen. Die unten folgende Abbildung veranschaulicht das Konzept von Cloud, Fog und Edge Computing. Während Fog Computing die Daten zwischen dem IoT-Endpunkt und der Cloud verarbeitet, werden die Daten beim Edge Computing in der Nähe der IoT-Endpunkte verarbeitet.

Cloud, Fog und Edge Computing



Quelle: Reza Vahidnia (2023)

Ähnlich wie beim Cloud Computing besteht auch ein Fog-Computing-System aus mehreren Komponenten, darunter die Infrastruktur, die Plattform, IaaS, PaaS und SaaS. Die folgende Abbildung veranschaulicht die technische Schichtenarchitektur einer Fog-Plattform. Beachten Sie, dass in dieser Architektur jedes Gerät mit Netzwerk-, Speicher- und Rechenkapazitäten zu einem Fog-Knoten werden kann. Fog-Knoten können miteinander auf Peer-to-Peer-Basis kommunizieren oder sie können einen Cluster bilden.

Schichtmodell des Fog Computings

Quelle: Reza Vahidnia (2023) basierend auf Atlam (2018)

### Physikalische Schicht und Virtualisierungsschicht

Diese Schicht umfasst verschiedene physische und virtuelle Knoten und Sensornetzwerke, die ihre Daten an die oberen Schichten senden.

### Überwachungsschicht

Diese Schicht überwacht den Energieverbrauch und alle von den verschiedenen Knoten ausgeführten Aufgaben. Außerdem überwacht sie den Status und die Leistung der in der Infrastruktur bereitgestellten Dienste und Anwendungen.

### Vorverarbeitungsschicht

Diese Schicht extrahiert aussagekräftige Daten, indem sie die von den IoT-Geräten erfassten Daten analysiert, filtert und aufbereitet.

### Temporäre Speicherschicht

Diese Schicht ist für die Zwischenspeicherung der vorverarbeiteten Daten zuständig, bevor die Daten an die Cloud übertragen werden. Sobald die Daten in die Cloud übertragen wurden, können sie aus dem Speicher dieser Schicht entfernt werden.

### Sicherheitsschicht

Auf dieser Ebene werden die Daten durch Integritätsmaßnahmen vor Manipulationen geschützt. Auch die Ver- und Entschlüsselung von Daten wird in dieser Schicht vorgenommen.

### Transportschicht

Die ausgewählten und vorverarbeiteten Daten werden über diese Schicht in die Cloud hochgeladen.

Fog Computing verkürzt zwar die Reaktionszeit von IoT-Systemen, spart Netzwerkbandbreite und bietet einen besseren Datenschutz, da Branchen und Unternehmen ihre Daten lokal analysieren können, hat aber auch seine Nachteile. Das Hinzufügen einer weiteren Berechnungsebene zwischen der Cloud und den IoT-Geräten erhöht den Stromverbrauch und die Komplexität des Systems, da die Verwaltung der Daten und die Planung von Aufgaben zwischen der Cloud und der Fog-Ebene normalerweise schwierig ist. Darüber hinaus erfordert die Speicherung und Berechnung der Daten in der Fog-Ebene eine Ver- und Entschlüsselung, was den Stromverbrauch und die Komplexität des Fog Computings weiter erhöht. Die Vor- und Nachteile von Fog Computing sind in der nachstehenden Tabelle zusammengefasst:

|  |  |
| --- | --- |
| Vor- und Nachteile von Fog Computing | |
| **Vorteile** | **Nachteile** |
| ✔ Es erhöht die Sicherheit und den Schutz der Daten, da die Daten das interne Netz nicht verlassen. | ✘ Es erfordert zusätzliche Sicherheitsmaßnahmen, um einige Angriffe wie Man-in-the-Middle-Angriffe abzuwehren. |
| ✘ Es spart Kosten, da weniger Daten in das Netz hochgeladen werden. | ✘ Es bietet keinen ausreichenden Schutz gegen Ausfall oder Missbrauch |
| ✘ Es spart Bandbreite, da weniger Datenverkehr in das Netz fließt. | ✘ Es erhöht den Wartungsaufwand, da die Speicherressourcen verteilt sind. |
| ✘ Es reduziert die Netzwerkverzögerung (Latenz) und erhöht die Reaktionszeit. | ✘ Es erhöht die Hardwarekosten, da zusätzliche Verarbeitungsressourcen benötigt werden. |
| ✘ IoT-Endpunkte können auch offline verfügbar sein. |  |

Quelle: Reza Vahidnia (2023) basierend auf fog-computing (2022)

Fog Computing ist nicht unbedingt für alle IoT-Einsatzfälle empfehlenswert, kann aber in den folgenden Szenarien nützlich sein:

* Bei Anwendungen wie Überwachungskameras, bei denen nicht alle Rohdaten in der Cloud gespeichert oder analysiert werden müssen.
* In unternehmenskritischen Anwendungen wie der Fahrzeug-zu-Fahrzeug-Kommunikation, wo eine geringe Latenzzeit entscheidend ist und eine Entscheidung sofort getroffen werden muss.
* Wenn eine große Anzahl verschiedener Dienste an verschiedenen Orten in einem großen geografischen Gebiet erbracht werden soll.
* Wenn die Daten der IoT-Geräte rigorosen Berechnungen und Verarbeitungen unterworfen werden.

### Herausforderungen beim Fog Computing im IoT

Der erfolgreiche Einsatz einer Fog-Computing-Lösung bringt viele Herausforderungen mit sich, von denen wir die folgenden hier erwähnen (Atlam, 2018):

* **Skalierbarkeit:** Fog-Ressourcen müssen in der Lage sein, auf eine große Anzahl von IoT-Geräten zu reagieren.
* **Komplexität:** Verschiedene IoT-Geräte stammen von unterschiedlichen Herstellern und unterstützen unterschiedliche Protokolle und Standards, was die Auswahl der optimalen Fog-Komponenten erschwert.
* **Dynamik:** Die dynamische Änderung des Arbeitsablaufes der IoT-Geräte erfordert, dass die Fog-Knoten ihre topologische Struktur und zugewiesenen Ressourcen automatisch neu konfigurieren.
* **Sicherheit:** Fog Computing ist in der Regel anfälliger und weniger sicher als Cloud Computing. Die Mobilität, die Heterogenität und die großflächige geografische Verteilung der Fog-Umgebung lassen die Anwendung der bestehenden Cloud-Sicherheits- und Datenschutzmechanismen nicht zu. Beim Cloud Computing besitzen die Dienstanbieter in der Regel die Rechenzentren. Beim Fog Computing hingegen sind verschiedene Ressourcen im Besitz unterschiedlicher Unternehmen, was die Implementierung von Sicherheitsmechanismen erschwert.
* **Ressourcenmanagement:** Fog-Knoten benötigen eine effiziente Verwaltung, da diese Netzwerkgeräte mit einer gewissen zusätzlichen Verarbeitungs- und Speicherleistung in der Regel weniger leistungsfähig sind als herkömmliche Server oder die Cloud.
* **Energieverbrauch:** Die Reduzierung des Stromverbrauchs in einer verteilten Fog-Umgebung kann eine schwierige Aufgabe sein.

### Fragen zur Selbstkontrolle

1. Erklären Sie bitte die Rolle der Überwachungsschicht im Schichtenmodell des Fog Computings.

Diese Schicht überwacht den Energieverbrauch und alle von den verschiedenen Knoten ausgeführten Aufgaben. Außerdem überwacht sie den Status und die Leistung der in der Infrastruktur bereitgestellten Dienste und Anwendungen.

1. Bitte wählen Sie das Szenario aus, in dem Fog Computing dem Cloud Computing vorgezogen wird.

* Einsatzkritische Anwendungen, bei denen eine sofortige Entscheidungsfindung erforderlich ist.
* Anwendungen mit hoher Latenzzeit, z.B. intelligente Zähler
* Anwendungen mit geringer Bandbreite, z. B. Temperaturmessungen
* Aktualisierung der Firmware der IoT-Geräte

1. Erläutern Sie bitte, warum Fog Computing anfälliger und weniger sicher ist als Cloud Computing.

Die Mobilität, die Heterogenität und die großflächige geografische Verteilung der Fog-Umgebung lassen die Anwendung der bestehenden Cloud-Sicherheits- und Datenschutzmechanismen nicht zu.

## 6.2 Bedrohungen für Cloud-Dienste im Internet der Dinge

Verschiedene Komponenten einer IoT-Lösung können von Angreifenden ausgenutzt werden. Die Sicherheitsbedrohungen können auf das IoT-Gerät (z. B. Knotenmanipulation, Social Engineering, Schlafentzug usw.) oder auf die Kommunikationskanäle abzielen, die verschiedene IoT-Komponenten miteinander verbinden (z. B. Sinkhole-Angriff, Sybil-Angriff, Verkehrsanalyse-Angriff usw.). Cyberkriminelle können die IoT-Systeme kompromittieren, indem sie die Schwachstellen der Webanwendungen und der Software zum Diebstahl von Anmeldedaten oder zum Versenden bösartiger Firmware-Updates ausnutzen. In der Schicht der Cloud-Dienste können böswillig Agierende die Cloud-Dienste kompromittieren, um bösartige Aktivitäten durchzuführen (z. B. Denial-of-Service, böswillige Insider usw.).

Bei der Nutzung von Cloud-Diensten haben Entwickelnde und Nutzende von IoT-Anwendungen keine vollständige Kontrolle über ihre Anwendungen und Daten. Dieser Mangel an Kontrolle erhöht die Sicherheits- und Datenschutzrisiken, die mit der Nutzung von Cloud-Diensten verbunden sind. Die fünf kritischsten Sicherheitsbedrohungen, die sich negativ auf Cloud-basierte Dienste für IoT-Anwendungen auswirken, sind folgende (Saini et al., 2022):

### Datenschutzverletzungen:

**SQL-Injektion**

Bösartige SQL-Codes werden zur Manipulation der Backend-Datenbank verwendet, um auf Daten zuzugreifen.

Datenschutzverletzungen treten auf, wenn Hacker:innen oder böswillige Nutzende sich illegal Zugang zu den in der Cloud gespeicherten oder verarbeiteten Daten verschaffen. **SQL-Injektion (Structured-Query-Language-Injektion)** gilt als der bekannteste Angriff, um Zugang zu den Daten zu erhalten. Da oftmals mehrere Anwendungen eine Datenbank gemeinsam nutzen, kann eine Schwachstelle in einer der Anwendungen Hacker:innen die Daten aller Anwendungen offenlegen.

### Datenverlust

Bei dieser Art von Bedrohung zerstören Angreifende oder eine Schadsoftware absichtlich die Daten. Auch Naturkatastrophen wie Brände, Erdbeben oder Überschwemmungen können zum Ausfall der Infrastruktur des Cloud Service Providers (CSP) und damit zu Datenverlusten führen. Um das Risiko eines Datenverlusts zu mindern, sollten CSPs daher regelmäßig Sicherungskopien ihrer Daten erstellen.

Der Schutz der Cloud-Daten liegt in der gemeinsamen Verantwortung von CSP und Kund:innen. Cloud-Benutzende können ebenfalls verantwortlich für den Verlust ihrer Daten sein. Wenn Cloud-Kund:innen beispielsweise ihre privaten oder öffentlichen Schlüssel für die Datenverschlüsselung verlieren, können sie ihre hochgeladenen und in der Cloud gespeicherten Daten nicht mehr entschlüsseln und nutzen.

**Anwendungsprogrammierschnittstelle (API)**

Ein Software-Vermittler, der die Kommunikation zwischen zwei Anwendungen erleichtert.

### Unsichere Schnittstellen und APIs

Die Kund:innen verwenden **Anwendungsprogrammierschnittstellen (APIs)**, um mit den Cloud-Diensten zu interagieren und diese zu verwalten. Eine unsichere und fehlerhafte Implementierung der Authentifizierung und des Kontrollzugriffs auf diese APIs (z. B. Offenlegung von Daten ohne Schutz der Vertraulichkeit) ermöglicht es Hacker:innen, die Cloud-Dienste anzugreifen. Die Metadaten von APIs machen es Cyberkriminellen leichter, Sicherheitsschwachstellen zu entdecken, da sie eine umfangreiche Angriffsfläche bieten (Korzeniowski, 2018). Die folgenden vier Aspekte sollten von den Cloud-Dienst-Anbietern berücksichtigt werden, um die APIs zu sichern (Korzeniowski, 2018):

* API-Schlüssel müssen von allen APIs verwendet werden, um sie zu sichern.
* Zusatzsoftware muss sorgfältig überwacht werden, da Hacker:innen die Verwendung offener Schnittstellen ausnutzen könnten.
* API-Schlüssel sollten nicht in einem Quelltext-Repository veröffentlicht werden.
* Die mit der Verwendung von APIs verbundenen Risiken sollten berücksichtigt werden.

### Denial-of-Service (DoS)

Bei dieser Art von Angriff versuchen Hacker:innen, Cloud-Dienste zu verlangsamen oder zu stoppen, indem sie eine große Menge an Cloud-Ressourcen wie Speicher, Bandbreite und Arbeitsspeicher verbrauchen. Wenn diese Angriffe von verschiedenen Quellen aus durchgeführt werden, spricht man von Distributed-Denial-of-Service (DDoS).

### Unzureichendes Design, unzureichende Planung und Fehlkonfiguration

Organisationen sollten mit der Cloud-Umgebung und den damit verbundenen Risiken vollständig vertraut sein, um zu verhindern, dass ungeeignete Anwendungen in die Cloud verlagert werden. Das Hochladen interner Kryptografie-, Netzwerküberwachungs- oder Störungsreaktionsdaten in die Cloud kann einige Probleme verursachen.

### Physische Sicherheitsbedrohungen

Die Cloud-Rechenzentren bestehen aus Hardwareressourcen wie Speicher-, Rechen- und Netzwerkkapazitäten und Infrastrukturen, die vor physischen Sicherheitsbedrohungen wie Feuer, Überschwemmung und Naturkatastrophen geschützt werden müssen.

### Fragen zur Selbstkontrolle

1. Erläutern Sie bitte anhand eines Beispiels, warum auch Cloud-Benutzende für den Schutz der Cloud-Daten verantwortlich sind.

Cloud-Benutzende können ebenfalls verantwortlich für den Verlust ihrer Daten sein. Wenn Cloud-Kund:innen beispielsweise ihre privaten oder öffentlichen Schlüssel für die Datenverschlüsselung verlieren, können sie ihre hochgeladenen und in der Cloud gespeicherten Daten nicht mehr entschlüsseln und nutzen.

## 6.3 Cloud-basierte Sicherheitsdienste

Cloud-basierte Sicherheitsdienste verbessern die Regelkonformität und mindern das Risiko von Cloud-Umgebungen, die in der Regel vielen verschiedenen Sicherheitsbedrohungen ausgesetzt sind. Es gibt keine Einzellösung, die das breite Spektrum komplexer Sicherheitsfragen abdecken kann. Daher wurden verschiedene Sicherheitsdienste so konzipiert, dass jeder Dienst einen bestimmten Bereich abdeckt. Diese Sicherheitsdienste werden üblicherweise von Drittanbietern übernommen. Die Auslagerung von Sicherheitsdiensten an Dritte bzw. an Anbieter von Managed Cloud Security Services hat viele Vorteile (Bonuccelli, 2022):

* Sicherheitsbedrohungen werden von Sicherheitsexpert:innen aufgespürt und bekämpft
* Organisationen werden angeleitet, Vorschriften besser einzuhalten
* Die IT-Zuständigen des Unternehmens können sich auf die Unterstützung ihrer Mitarbeitenden konzentrieren und müssen sich nicht um Sicherheitsvorfälle kümmern.

### Arten Cloud-basierter Sicherheitsdienste

Im Folgenden sind einige der gängigsten Cloud-basierten Sicherheitsdienste aufgeführt (Bonuccelli, 2022):

#### Data Loss Prevention

Data Loss Prevention (DLP, Schutz vor Datenverlust) ist eine Zusammenstellung von Tools und Technologien, die zum Schutz sensibler Daten wie Kreditkarten- und Gesundheitsdaten vor unbefugtem Zugriff eingesetzt werden. DLP-Tools verhindern, dass Mitarbeitende sensible und vertrauliche Geschäftsinformationen des Unternehmensnetzwerks nach außen versenden, indem sie die übertragenen Daten mithilfe fortschrittlicher Algorithmen überwachen, E-Mails mit bösartigen Anhängen oder verdächtigen Links blockieren und Regeln zur Einhaltung der Unternehmensrichtlinien anwenden.

DLP schützt die Daten auch, während sie von autorisierten Benutzenden in Endgeräten und Anwendungen verwendet werden, bei der Übertragung über ein Netzwerk (durch Verschlüsselung der Informationen) oder im Ruhezustand, wenn sie in der Cloud, in Datenbanken und auf Endgeräten gespeichert sind (durch Verschlüsselung, Zugriffskontrolle und Richtlinien zur Datenaufbewahrung) (Spanning Cloud Apps, 2022).

Im Folgenden finden Sie einige bewährte Verfahren für DLP (Spanning Cloud Apps, 2022):

* **Ziele festlegen:**Der Zweck der Anwendung von DLP sollte klar definiert werden, um die Arten von Lösungen zu bestimmen, die in der DLP-Strategie implementiert werden sollen. So sind beispielsweise die bessere Sichtbarkeit von Informationen, der Schutz geistigen Eigentums oder die Einhaltung gesetzlicher Vorschriften einige Ziele, die unterschiedliche DLP-Strategien erfordern.
* **Daten identifizieren und klassifizieren:**Kritische Geschäftsdaten, wie z. B. Finanzdaten, sollten identifiziert und entsprechend ihrer Wichtigkeit klassifiziert werden.
* **Daten-Sicherheitsrichtlinien definieren:**Damit die DLP in der Lage ist, sensible Daten zu analysieren und zu blockieren, um ihre Übertragung an unbefugte Benutzende zu verhindern, sollte ein umfassender Satz von Sicherheitsregeln und -richtlinien entwickelt und im gesamten Unternehmen eingeführt werden.
* **Zugriff verwalten:**Es sollten Rollen für Benutzende und Berechtigungsstufen definiert werden, um den Zugang zu sensiblen Informationen zu beschränken.

#### Identity and Access Management (IAM, Identitäts- und Zugangsmanagement)

IAM setzt Berechtigungs- und Zugriffsrichtlinien durch und definiert die Zugriffsstufe der verschiedenen Benutzenden auf Cloud-Dienste. Im Wesentlichen legt IAM fest, wer auf die Cloud-Ressourcen zugreifen kann, welche Komponenten zugriffsberechtigt sind, welche Aktionen erlaubt und verweigert werden und wann der Zugriff auf Cloud-Ressourcen möglich ist. Zum Beispiel sollten Nicht-Administrator:innen keinen Zugriff auf das Erstellen oder Löschen von Instanzen haben.

Die IAM-Richtlinien können entweder identitätsbasiert oder ressourcenbasiert sein. Die identitätsbasierten Richtlinien legen die Berechtigungen für eine Identität wie einen Benutzenden, eine Gruppe oder eine Rolle fest. Die ressourcenbasierten Richtlinien bestimmen, wer Zugriff auf eine Ressource hat und welche Aktionen er/sie mit dieser Ressource durchführen kann.

Arten von IAM

Quelle: Reza Vahidnia (2023) basierend auf Access policies (2023).

#### Websicherheit

Web-Sicherheitslösungen ermöglichen es Netzwerkadministrierenden, die Verbindungen zwischen den IoT-Geräten und dem Internet zu sichern und sie vor Cyberangriffen zu schützen.

#### Intrusionserkennung

Algorithmen zur Mustererkennung werden eingesetzt, um Bedrohungen zu identifizieren, verdächtige Aktivitäten im ein- und ausgehenden Datenverkehr zu überwachen und Intrusionen zu erkennen.

### Fragen zur Selbstkontrolle

1. Erläutern Sie bitte die beiden Arten von Identity and Access Management zur Sicherung der Cloud.

Die identitätsbasierten Richtlinien legen die Berechtigungen für eine Identität wie einen Benutzenden, eine Gruppe oder eine Rolle fest. Die ressourcenbasierten Richtlinien bestimmen, wer Zugriff auf eine Ressource hat und welche Aktionen er/sie mit dieser Ressource durchführen kann.

1. Bitte nennen Sie drei Vorteile, die erklären, warum die Sicherheitsdienste von Dritten übernommen werden.

Sicherheitsbedrohungen werden von Sicherheitsexpert:innen aufgespürt und bekämpft.

Organisationen werden angeleitet, Vorschriften besser einzuhalten.

Die IT-Zuständigen des Unternehmens können sich auf die Unterstützung ihrer Mitarbeitenden konzentrieren und müssen sich nicht um Sicherheitsvorfälle kümmern.

## 6.4 Absicherung der Cloud-Lösung

Die Sicherheit gilt in vielen Organisationen als das größte Problem bei der Einführung von Cloud Computing. Um eine Cloud-Lösung zu sichern, können verschiedene Maßnahmen ergriffen werden. Dazu gehören (cloud-security 10 ways, 2022):

1. Besonders sensible Daten sollten auf einem sicheren lokalen Speicher und nicht in der Cloud gespeichert werden. Wenn die vertraulichen Daten in der Cloud kompromittiert werden, kann das gesamte Unternehmen oder die Organisation in Gefahr sein.
2. Eine Naturkatastrophe oder eine versehentliche Beschädigung kann zum Verlust aller in der Cloud gespeicherten Daten führen. Es wird daher dringend empfohlen, lokale Backups aller Cloud-Daten zu erstellen, um eine Ersatzkopie zu haben.
3. Die Verwendung desselben leicht zu merkenden Passworts für mehrere Konten und Plattformen erhöht das Hacking- und Diebstahlsrisiko der Cloud-Daten. Um das Hacken von Daten zu verhindern, sollten für jedes Cloud-Konto starke und eindeutige Passwörter verwendet werden. Die Anbieter von Cloud-Diensten sollten von den Nutzenden verlangen, dass sie ihre Passwörter regelmäßig ändern.

Der Einsatz von Multi-Faktor-Authentifizierung (MFA) zusätzlich zu normalen Passwörtern erfordert, dass Mitarbeitende und Kontonutzende ihre Mobiltelefone oder E-Mail-Konten als weitere Vertrauensquelle nutzen und den an ihr Telefon und ihren Computer gesendeten Code eingeben. MFA stoppt automatisierte Hacking-Versuche und verbessert die Passwortsicherheit.

FIDO (Fast Identity Online) ist ein Beispiel für einen Authentifizierungsstandard, der auf Kryptografie mit öffentlichen Schlüsseln basiert. Es bietet eine bessere Benutzererfahrung als die bestehenden One-Time-Password-Lösungen (OTP-Lösungen). FIDO ermöglicht es Nutzenden, sich mit ihren Zugangsdaten anzumelden, die gegen Phishing geschützt sind, um auf mehrere Websites und Anwendungen zuzugreifen. Die Zugangsdaten können über mehrere Geräte hinweg synchronisiert oder an eine Plattform gebunden werden (What is FIDO, 2022)**.**

**NFC**

Eine Art von Funktechnologie, die für die Kommunikation von Geräten mit einem Abstand von wenigen Zentimetern verwendet wird.

Die meisten MFA-Methoden beruhen auf einer der drei folgenden Arten von Zusatzinformationen:

* Wissen: Informationen, die den Nutzenden bekannt sind, wie eine PIN oder ein Passwort
* Besitz: Gegenstände, welche die Nutzenden besitzen, wie eine **NFC**-Karte (**Near-Field-Communication**-Karte)
* Inhärenz: Eigenschaften, die zu den Nutzenden gehören, wie biometrische Daten (z. B. Fingerabdrücke oder Gesichtserkennung)

Multi-Faktor-Authentifizierung



Quelle: Reza Vahidnia (2023)

1. Strenge Zugangskontrollen, die sich am tatsächlichen Bedarf und nicht an der Position orientieren, schränken den Zugriff auf die Benutzenden ein, die ihn benötigen.
2. Durch die Verschlüsselung der Daten vor dem Hochladen in die Cloud wird verhindert, dass unbefugte Benutzende darauf zugreifen können. Nur Benutzende mit dem entsprechenden Entschlüsselungscode können die Daten lesen.
3. Die Verwendung von Anti-Malware-Tools kann äußerst hilfreich sein, um eine Gefährdung der mit der Cloud verbundenen Geräte zu vermeiden.
4. Durch die regelmäßige Prüfung der Sicherheit der Cloud-Dienste kann festgestellt werden, ob die Sicherheitsmaßnahmen in der Cloud wie versprochen funktionieren oder im Laufe der Zeit nachgelassen haben.
5. Trotz starker Sicherheitsmechanismen kann ein Cloud-System aufgrund menschlicher Nachlässigkeit gehackt werden. Die richtige Schulung der Nutzenden über die Sicherheit in der Cloud, um Angriffe wie Phishing zu erkennen, kann dazu beitragen, die Cloud-Lösungen zu sichern.
6. Nicht alle Anbieter von Cloud-Diensten verfügen über strenge Sicherheitsmaßnahmen. Die Auswahl des richtigen Cloud-Anbieters mit fortschrittlicher Cloud-Sicherheit, wie z. B. einer ausgefeilten Verwaltung von Anmeldeinformationen und Verschlüsselungstools auf Dateiebene, ist für die Sicherheit vieler Cloud-Lösungen unerlässlich.

### Fragen zur Selbstkontrolle

1. Erläutern Sie bitte, warum empfohlen wird, lokale Backups von allen Cloud-Daten zu erstellen.

Eine Naturkatastrophe oder eine versehentliche Beschädigung kann zum Verlust aller in der Cloud gespeicherten Daten führen.

1. Bitte wählen Sie aus, welche Option den Zweck strenger Zugriffskontrollen beschreibt.

* Beschränkung des Zugriffs auf die Benutzenden, die ihn benötigen
* Einsparung von Bandbreite
* Steigerung der Leistung von Cloud-Diensten
* Verringerung der Wartungskosten der Cloud

Zusammenfassung

IoT-Lösungen können von Fog Computing profitieren, um Bandbreite und Latenz des Systems zu reduzieren. IoT-Lösungen können auch Cloud-Dienste in Form von SaaS, PaaS oder IaaS nutzen, um die Betriebskosten zu senken und auf die von verschiedenen Sensoren in unterschiedlichen geografischen Gebieten erfassten Daten zuzugreifen. Neben den vielen bedeutenden Vorteilen von Cloud-Diensten kann jedoch jede Sicherheitsverletzung das gesamte IoT-Ökosystem gefährden. Daher sollten vor der Entwicklung einer Cloud-basierten Lösung die Schwachstellen der Cloud und die erforderlichen Sicherheitsmechanismen zum Schutz der IoT-Daten berücksichtigt werden.

Die kritischsten Sicherheitsbedrohungen, die Cloud-basierte Dienste für IoT-Anwendungen beeinträchtigen können, sind Datenschutzverletzungen, Datenverlust, unsichere Schnittstellen und APIs, Denial-of-Service (DoS) sowie physische Sicherheitsbedrohungen. Um diesen Sicherheitsbedrohungen zu begegnen, wurden verschiedene Cloud-basierte Sicherheitsdienste entwickelt. Der wichtigste Cloud-basierte Sicherheitsdienst ist Data Loss Prevention. Dabei handelt es sich um eine Reihe von Tools und Technologien zum Schutz vertraulicher Daten vor unbefugtem Zugriff. Identity and Access Management (IAM), E-Mail-Sicherheit, Web-Sicherheit und Intrusionserkennung sind einige weitere Cloud-basierte Sicherheitsdienste.

Darüber hinaus können zur Sicherung einer Cloud-Lösung verschiedene Maßnahmen ergriffen werden, wie z. B. die Speicherung sensibler Daten auf einem sicheren lokalen Speicher, die Erstellung lokaler Backups, die Wahl starker Passwörter und die Verwendung einer Multi-Faktor-Authentifizierung.

# Lektion 7 – Big Data und Künstliche Intelligenz

**Lernziele**

Nach dem Abschluss dieser Lektion werden Sie...

... die Begriffe Big Data und Künstliche Intelligenz beschreiben können.

... die Unterschiede zwischen überwachten und unüberwachten Algorithmen des Maschinenlernens erklären können.

... zwischen Regression und Klassifizierung unterscheiden können.

... die Anwendung des Maschinenlernens für die IoT-Sicherheit erläutern können.

... die wichtigsten überwachten und unüberwachten Algorithmen des Maschinenlernens identifizieren können.

# 7. Big Data und Künstliche Intelligenz

**MapReduce**

Ein Programmiermodell zur Verarbeitung von Big Data durch Filtern und Sortieren (Map-Stufe) und Zusammenfassen von Daten (Reduce-Stufe).

## Einführung

Die große Anzahl von IoT-Geräten erzeugt riesige Datenmengen in unterschiedlichen Strukturen und Formaten, die mit herkömmlichen Datenspeicher- und Analysetools nicht verarbeitet werden können. Darüber hinaus ist die Analyse dieser riesigen Datenmengen zur Erkennung von Mustern und zur Gewinnung nützlicher Erkenntnisse keine leichte Aufgabe und kann nicht manuell durchgeführt werden. Aus diesem Grund müssen wir uns für den Umgang mit IoT-Daten mit zwei wichtigen Konzepten vertraut machen: mit Big Data und künstlicher Intelligenz (KI).

Big Data und künstliche Intelligenz werden in der Regel im Zusammenhang miteinander verwendet, erfüllen aber unterschiedliche Aufgaben. Während sich Big Data auf die Informationen bezieht, geht es bei der künstlichen Intelligenz um die Verarbeitung dieser Daten.

### Big Data

Große und komplexe Datensätze, die aus verschiedenen Quellen stammen und mit herkömmlichen Datenverwaltungs- und Analysetools nicht verwaltet und bearbeitet (d. h. erfasst, gespeichert, analysiert und visualisiert) werden können, werden auch als Big Data bezeichnet. Für die Speicherung und Verarbeitung von Big Data sind spezielle Datenverarbeitungstools wie Apache Hadoop erforderlich, die in der Regel auf mehreren Rechnern und Servern verteilt arbeiten. Apache Hadoop besteht aus einer Reihe von Open-Source-Softwareprogrammen für die verteilte Speicherung und Verarbeitung großer Datenmengen, die den MapReduce-Algorithmus verwenden.

Big Data wird in der Regel durch fünf Faktoren beschrieben, die im Englischen als 5 Vs bekannt sind.

5 Faktoren von Big Data

Quelle: Reza Vahidnia (2023)

#### Volumen (Volume)

Das Volumen beschreibt die enorme Datenmenge, die von verschiedenen Datenpunkten und -quellen generiert wird und die sogar die Terabyte-Grenze überschreiten kann.

#### Geschwindigkeit (Velocity)

Die Geschwindigkeit beschreibt die Rate, mit der Daten produziert und verarbeitet werden. Um in Echtzeit auf Ereignisse reagieren zu können, sind sehr schnelle Datenanalysetools erforderlich.

#### Vielfalt (Variety)

Vielfalt bezieht sich auf die große Anzahl verschiedener Datentypen. Herkömmliche Datenverarbeitungsprogramme konnten nur strukturierte Daten (zweidimensionale Tabellen) verarbeiten. Die Datentypen von Big Data sind jedoch vielfältiger und können strukturiert (d. h. sie haben eine definierte Länge und ein definiertes Format), unstrukturiert (d. h. sie können nicht in der herkömmlichen Zeilen- und Spaltenstruktur der relationalen Datenbanken gespeichert werden) oder halbstrukturiert (d. h. sie sind semiorganisiert) sein.

#### Wert (Value)

Der Wert gibt an, welcher Teil der Daten in einer riesigen Menge von Big Data nützliche Erkenntnisse liefern kann. Data-Mining-Tools werden benötigt, um die relevanten Daten aus einem großen Datenmeer zu extrahieren.

#### Wahrhaftigkeit (Veracity)

Wahrhaftigkeit bezieht sich auf die Unsicherheit, Korrektheit und Vertrauenswürdigkeit der Daten.

### Künstliche Intelligenz

Künstliche Intelligenz (KI) bezieht sich auf ein Wissenschaftsgebiet, das sich mit der Entwicklung von Computern befasst, die in der Lage sind, zu lernen, zu argumentieren und auf eine Art und Weise zu handeln, die normalerweise menschliche Intelligenz erfordert, oder große Datenmengen verarbeiten können, die von Menschen nicht analysierbar sind (Google, 2021). KI ist ein interdisziplinäres Gebiet, das andere Wissenschaften wie Datenwissenschaft, Informatik, Elektrotechnik und Computertechnik, Neurowissenschaften, Linguistik, maschinelles Sehen, Verarbeitung natürlicher Sprache und sogar Philosophie und Psychologie umfasst.

**Deep Learning**

Eine Untergruppe des maschinellen Lernens, die sich bei der Gewinnung bestimmter Arten von Wissen wie ein Mensch verhält.

KI wird als eine Reihe von Technologien betrachtet, darunter maschinelles Lernen (ML) und **Deep Learning**, die zur Datenanalyse, zur Vorhersage von Ereignissen, zur Kategorisierung von Objekten, zur Verarbeitung natürlicher Sprache, zum intelligenten Abrufen von Daten und für viele weitere Anwendungen eingesetzt werden. Mit Hilfe der KI sind selbstlernende Computersysteme in der Lage, eine Vielzahl fortgeschrittener und komplexer Funktionen auszuführen, wie z. B. gesprochene und geschriebene Sprache zu verstehen, Daten zu analysieren, Schlussfolgerungen zu ziehen und Empfehlungen und Entscheidungen effizienter zu treffen als Menschen.

Privatpersonen und Unternehmen können bei der Prozessautomatisierung und der Erkenntnisgewinnung aus großen Datensätzen von der KI profitieren. Die KI-Einsatzfälle reichen von autonomen Drohnen bis zu persönlichen Assistenzsystemen. Wir benutzen KI-Systeme in unserem Alltagsleben, denn beispielsweise funktionieren alle persönlichen Assistenzsysteme wie Siri, Alexa und Bixby mit KI. Ein weiteres Beispiel für KI in unserem täglichen Leben ist, wenn uns beim Besuch von Websites ein Produkt oder ein Video empfohlen wird, das uns interessiert.

Vorteile von AI

Quelle: Reza Vahidnia (2023) basierend auf Google (2021).

#### In den vergangenen Jahren haben Cyberkriminelle damit begonnen, KI für Sicherheitsangriffe zu nutzen. Umgekehrt nutzen Cybersicherheitsexpert:innen ebenfalls KI, um IoT-Systeme dynamisch vor Sicherheitsbedrohungen zu schützen. So können sie beispielsweise Intrusionen erkennen, indem sie die Verkehrsmuster analysieren und nach böswilligen Aktivitäten suchen (Kuzlu et al., 2021).

#### Derzeit ist der Einsatz von KI zur Bekämpfung kleinerer Sicherheitsbedrohungen noch recht teuer und ressourcenintensiv. Daher ist es eher für Unternehmen mit großen Netzwerken oder umfangreichen Anwendungen, wie z. B. Smart City, praktikabel und vorteilhaft, KI zum Schutz ihrer IoT-Systeme einzusetzen. In naher Zukunft werden KI-Cybersicherheitsmaßnahmen jedoch auch zum Schutz kleinerer Einsatzfälle – wie intelligenter Häuser oder selbstfahrender Fahrzeuge – eingesetzt werden, um Sicherheitsbedrohungen schnell zu erkennen Kuzlu et al., 2021.

#### Einige der KI-basierten Cyberangriffe und Gegenmaßnahmen sind die folgenden Kuzlu et al., 2021:

#### Schwachstellenerkennung

#### Sowohl Cyberkriminelle als auch Sicherheitsfachleute können KI nutzen, um automatisch Schwachstellen in einem IoT-System zu entdecken, allerdings für unterschiedliche Zwecke. Cyberangreifende verwenden KI, um Schwachstellen aufzuspüren und sie schneller auszunutzen als Entwickelnde sie beheben können. Im Gegenzug nutzen Entwickelnde und Cybersecurity-Fachkräfte KI bei der Suche nach und Behebung von Schwachstellen.

#### Eingabeangriffe

#### Ein Eingabeangriff liegt vor, wenn Angreifende das Muster der Eingabedaten verändern (z. B. indem sie einem Bild Rauschen hinzufügen, um den KI-Algorithmus in die Irre zu führen), so dass das KI-System verwirrt wird und eine falsche Ausgabe erzeugt.

#### Datenvergiftung/Injektion falscher Daten

Datenvergiftungsangriffe sind den Eingabeangriffen ziemlich ähnlich, mit dem Unterschied, dass sie ein anderes Ziel verfolgen. Der Hauptzweck von Datenvergiftungsangriffen besteht darin, den Trainingsprozess der KI zu stören, indem die Eingabedaten über einen langen Zeitraum verändert werden, so dass die KI die Ausgabe für bestimmte Eingaben nicht vorhersagen kann. In einem militärischen Einsatzfall kann das KI-System beispielsweise nicht in der Lage sein, die feindlichen Drohnen zu erkennen, wenn es während des Trainings mit falschen Daten versorgt wird. Datenvergiftung und die Einspeisung falscher Daten können auch die Fähigkeiten eines KI-Systems für vorausschauende Wartungsanwendungen lahmlegen. Angreifende können die folgenden drei Vergiftungsmethoden verwenden, um ein KI-System zu schädigen:

**Föderales Lernen**

Eine KI-Trainingsmethode, die gleichzeitig den Datenschutz von Einzelpersonen gewährleistet.

* **Datensatzvergiftung:** Verfälschung des Trainingsdatensatzes durch Aufnahme falscher oder falsch beschrifteter Informationen
* **Algorithmusvergiftung:** Bei diesen Angriffen, die beim **föderalen Lernen** eine wichtige Rolle spielen, wird das endgültige Modell vergiftet, weil der Algorithmus die von Angreifenden manipulierten Daten wie Benutzerdaten verwendet.
* **Modellvergiftung:** Bei dieser Art von Angriff ersetzen Cyberkriminelle das legitime KI-Modell oder die legitimen KI-Daten durch ein vergiftetes Modell in dem System, in dem die Modelle und Daten gespeichert sind.

#### Arten von Künstlicher Intelligenz

Je nach Entwicklungsstufe kann die KI auf unterschiedliche Weise organisiert werden. Die bekanntesten AI-Entwicklungsstufen sind folgende (Kumar, 2018):

* **Reaktive Maschinen:** Diese begrenzte Art von KI, die weder über ein Gedächtnis verfügt noch aus neuen Datensätzen lernen kann, reagiert nur auf der Grundlage ihrer programmierten Regeln. Ein Beispiel für eine reaktive Maschine ist Deep Blue von IBM, die 1997 den Schachweltmeister Garry Kasparov besiegen konnte (Google, 2021).
* **Systeme mit begrenztem Speicher (Limited Memory):** In dieser KI-Entwicklungsstufe werden künstliche neuronale Netze oder andere Trainingsmodelle verwendet, die sich selbst verbessern. Ein Beispiel für KI mit begrenztem Speicher ist Deep Learning, ein Teilbereich des maschinellen Lernens.
* **Systeme mit eigenem Bewusstsein (Theory of Mind):** Diese Art von KI zielt darauf ab, den menschlichen Verstand nachzuahmen, indem sie menschenähnliche Entscheidungsfähigkeiten bereitstellt. Theory-of-Mind-KI ist noch nicht verwirklicht, aber an der Ermöglichung wird intensiv geforscht. Dann wird sie in der Lage sein, in sozialen Situationen genauso zu reagieren wie ein Mensch, dazu gehört zum Beispiel auch das Erkennen und Abspeichern von Emotionen.
* **Systeme mit Selbstwahrnehmung (Self-aware):**In dieser weiter fortgeschrittenen, noch nicht realisierten Form der KI werden sich die Maschinen ihrer Existenz bewusst sein und über die emotionalen und intellektuellen Fähigkeiten eines Menschen verfügen.

Um KI zu realisieren, müssen Computer trainiert werden, damit sie sich mit der Zeit weiterentwickeln und bessere Entscheidungen treffen können. Das maschinelle Lernen ist eine Untergruppe der KI, bei der Trainingsdaten verwendet werden, um einen Algorithmus zu trainieren und dadurch Ergebnisse zu erzielen. Im Allgemeinen werden beim maschinellen Lernen drei verschiedene Modelle verwendet, und zwar überwachtes Lernen, unüberwachtes Lernen und verstärkendes Lernen (Reinforcement Learning).

Algorithmen des maschinellen Lernens haben viele Anwendungen für die Sicherung von IoT-Anwendungen. Die bestehenden Sicherheitsmechanismen wie Verschlüsselung, Zugangskontrolle und Authentifizierung reichen möglicherweise nicht aus, um die komplexen Sicherheitsbedrohungen für IoT-Geräte und -Netze zu bewältigen. Hier können Algorithmen des maschinellen Lernens helfen, die Systeme besser abzusichern. In den nächsten Unterlernzyklen werden die überwachten und unüberwachten Algorithmen des maschinellen Lernens näher erläutert und einige Anwendungen solcher Techniken für die IoT-Sicherheit erörtert.

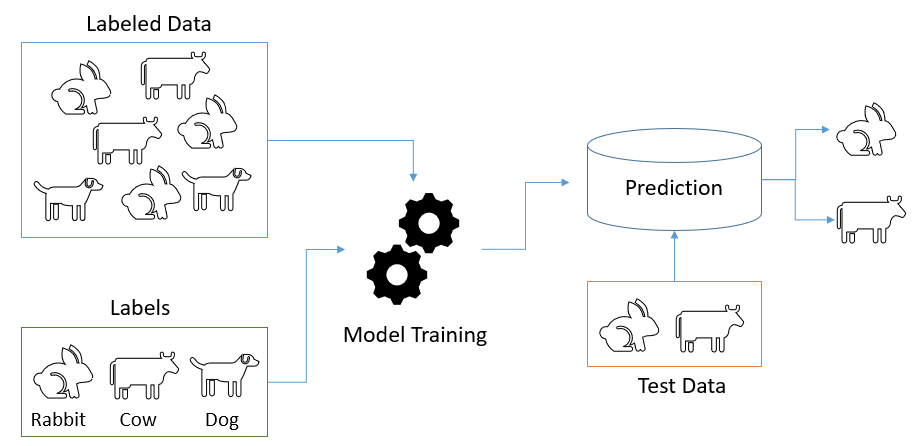
## 7.1 Überwachtes Lernen

Beim überwachten maschinellen Lernen werden beschriftete Trainingsdaten (markierte Daten mit bekannter Ausgabe) als „Überwacher“ verwendet, um Maschinen so zu trainieren, dass sie die Ausgaben eines Systems für neue Daten korrekt vorhersagen können. Das Konzept des überwachten Lernens kann mit dem Lernprozess in einem Klassenzimmer verglichen werden: Schüler:innen (Maschinen) werden von einer Lehrperson (beschriftete Daten) unterrichtet (trainiert) und erhalten die richtigen Antworten (Output), so dass sie anschließend in der Lage sind, die Prüfungsfragen zu beantworten (den Output für neue Daten vorherzusagen).

Der Hauptzweck des überwachten maschinellen Lernens besteht darin, eine Zuordnungsfunktion zu finden, welche die Beziehung zwischen der Eingabevariablen (X) und der Ausgabevariablen (Y) angeben kann. Überwachtes Lernen wird häufig eingesetzt, um Betrug zu erkennen, Spam auszufiltern und Bilder zu klassifizieren.

Sobald die Maschinen mit den markierten Datensätzen trainiert sind, wird ein Modell erstellt, das die Eingangs- und Ausgangsvariablen zueinander in Beziehung setzt. Dieses Modell wird dann mit Testdaten getestet, die eine Teilmenge des Trainingsdatensatzes darstellen. Schließlich wird das validierte Modell zur Vorhersage der Ausgabe des Systems für beliebige andere Daten verwendet. Die folgende Abbildung veranschaulicht die Funktionsweise des überwachten Lernens.

Überwachtes Lernen



Quelle: Reza Vahidnia (2023) basierend auf Supervised machine learning (2021)

Angenommen, es gibt einen Datensatz mit Bildern verschiedener Tiere, darunter Kaninchen, Kühe und Hunde. Der erste Schritt beim überwachten Lernen besteht darin, das Modell für jedes Tierbild zu trainieren. Nachdem das Modell trainiert wurde, wird ein Testdatensatz verwendet, um die Bilder zu identifizieren und die Zuverlässigkeit des Modells zu überprüfen. Nach dem Validierungsprozess ist die Maschine bereit, neue Bilder zu erkennen und festzustellen, ob es sich um ein Bild einer Kuh, eines Hundes oder eines Kaninchens handelt.

Nachfolgend sind die für das überwachte maschinelle Lernen erforderlichen Schritte aufgeführt:

1. Bestimmen des Trainingsdatensatztyps.
2. Sammeln der beschrifteten Trainingsdaten.
3. Aufteilen der Daten in drei Datensätze: Trainings-, Test- und Validierungsdatensatz.
4. Definition der Eingangsmerkmale des Trainingsdatensatzes, damit das Modell die Ausgabe vorhersagen kann.
5. Auswahl eines geeigneten Algorithmus wie Entscheidungsbaum oder Support Vector Machine für das Modell.
6. Ausführen von Algorithmen mit dem Trainingsdatensatz, um die Ergebnisse zu validieren.
7. Bewertung der Genauigkeit des Modells anhand des Testdatensatzes.

Die Vor- und Nachteile von überwachtem Lernen sind in der nachstehenden Tabelle zusammengefasst.

|  |  |
| --- | --- |
| Vor- und Nachteile de überwachten Lernens | |
| **Vorteile** | **Nachteile** |
| ✔ Die Ausgabe kann basierend auf früheren Erfahrungen erkannt werden. | ✘ Es ist für die Bewältigung komplexer Aufgaben nicht geeignet. |
| ✔ Es gibt eine genaue Vorstellung von den Objektklassen. | ✘ Es kann nicht die richtige Ausgabe vorhersagen, wenn die Test- und Trainingsdatensätze unterschiedlich sind. |
| ✔ Verschiedene reale Probleme wie die Erkennung von Betrug und die Ausfilterung von Spam können durch überwachtes Lernen gelöst werden. | ✘ Für das Training werden viel Rechenzeit und viele Ressourcen benötigt. |
|  | ✘ Eine genaue Vorstellung von den Objektklassen ist erforderlich. |

Quelle: Reza Vahidnia (2023) basierend auf Supervised machine learning (2021)

### Algorithmen des überwachten Lernens

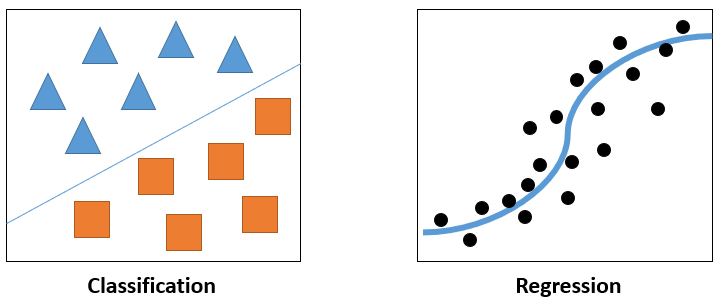
Die nachstehende Abbildung zeigt verschiedene Algorithmen des überwachten Lernens in den beiden Hauptkategorien Regression und Klassifizierung.

Arten von Algorithmen des überwachten Lernens

Quelle: Reza Vahidnia (2023) basierend auf Supervised machine learning (2021)

Sowohl Regressions- als auch Klassifizierungsalgorithmen werden mit beschrifteten Datensätzen trainiert, um Vorhersagen treffen zu können. Der Hauptunterschied zwischen ihnen besteht darin, dass Regressionsalgorithmen zur Vorhersage von kontinuierlichen Werten wie Wetter, Temperatur, Preis usw. verwendet werden, während Klassifizierungsalgorithmen zum Klassifizieren und Vorhersagen diskreter Werte wie wahr oder falsch, männlich oder weiblich, etc. dienen.

Regression versus Klassifizierung

****

Quelle: Reza Vahidnia (2023)

### **Regression**

Wenn eine Beziehung zwischen den Eingangs- und Ausgangsvariablen besteht, werden die Regressionsalgorithmen zur Vorhersage kontinuierlicher Variablen wie Markttrends oder Wettervorhersagen verwendet. Der Zweck der Regression besteht darin, die am besten passende Linie zu finden, welche den Ausgang, z. B. die Immobilienpreise, am genauesten vorhersagen kann. Einige der wichtigsten Regressionsalgorithmen sind die folgenden:

#### Lineare Regression

Die lineare Regression, welche die lineare Beziehung zwischen einer abhängigen Variablen und einer einzigen oder mehreren unabhängigen Variablen mit einer geneigten geraden Linie darstellt, ist einer der einfachsten und beliebtesten Regressionsalgorithmen, der typischerweise für die Vorhersage kontinuierlicher Variablen wie Umsatz, Alter oder Preis verwendet wird.

#### Regressionsbäume

Regressionsbäume sind eine Unterart von Entscheidungsbäumen, bei der die Zielvariablen in den Blättern kontinuierliche Variablen anstelle von Klassenbezeichnungen sein können (procedures regression trees, 2022). Die Verwendung von Regressionsbäumen hilft bei der Identifizierung von Ereignissen, die mit ihrem möglichen Ergebnis auftreten könnten. Sie helfen auch dabei, die beste Entscheidung zu treffen und diese zu erklären.

#### Nichtlineare Regression

Im Gegensatz zur linearen Regression, bei der die Beziehung von Eingangs- und Ausgangsvariablen durch eine gerade Linie dargestellt wird, wird bei der nichtlinearen Regression der Zusammenhang zwischen den Eingangs- und Ausgangsdaten durch eine nichtlineare mathematische Funktion ausgedrückt. Die zur Beschreibung der besten Anpassungskurve verwendete Kennzahl ist die Summe der Quadrate der Fehler (Differenz zwischen den Ausgangsbeobachtungen und der Anpassungskurve), die so klein wie möglich sein muss.

#### Bayessche Lineare Regression

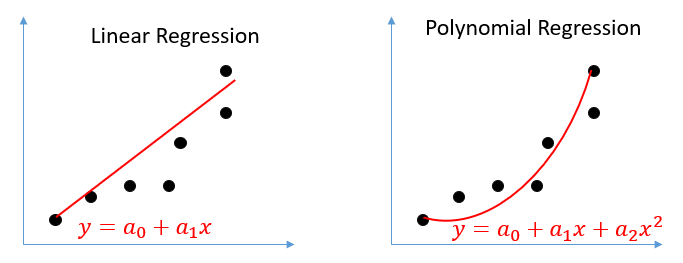
Bei der normalen linearen Regression werden die exakten Werte für die Gewichte und Abweichungen so gewählt, dass die mittlere quadratische Fehlerfunktion minimiert wird. Bei der Bayesschen linearen Regression werden anstelle von exakten Werten für die Gewichte und Verzerrungen deren Wahrscheinlichkeiten im Modell verwendet, so dass die Unsicherheit der Parameter berücksichtigt wird.

Beispielsweise können Bayessche Algorithmen frühere Verkehrsinformationen verwenden, um die Wahrscheinlichkeit eines Angriffs auf den Netzverkehr zu bewerten. Diese Fähigkeit ermöglicht es den Bayesschen Algorithmen, DoS-Angriffe, Netzwerk-Intrusionen und Anomalien zu erkennen (Al-Garadi et al., 2020).

#### Polynomische Regression

Bei der polynomischen Regression, bei der es sich im Grunde um ein lineares Modell mit einigen Modifikationen zur Verbesserung der Genauigkeit des Modells handelt, wird die Beziehung zwischen der abhängigen Variable y und der unabhängigen Variable x durch ein Polynom n-ten Grades modelliert. Der Unterschied zwischen dem linearen und dem polynomischen Modell ist in der folgenden Abbildung dargestellt:

Lineare Regression versus Polynomische Regression



Quelle: Reza Vahidnia (2023)

### **Klassifizierung**

Der Zweck von Klassifizierungsalgorithmen besteht darin, anhand von Trainingsdaten eine Abbildungsfunktion zu finden, mit deren Hilfe Eingabevariablen auf diskrete Ausgabevariablen abgebildet und die Daten auf der Grundlage verschiedener Parameter verschiedenen Klassen zugeordnet werden können. So können beispielsweise Klassifizierungsalgorithmen verwendet werden, um Spam-E-Mails zu erkennen und in einen separaten Ordner zu verschieben. Einige der bekanntesten Klassifizierungsalgorithmen des maschinellen Lernens sind die folgenden:

#### Entscheidungsbäume

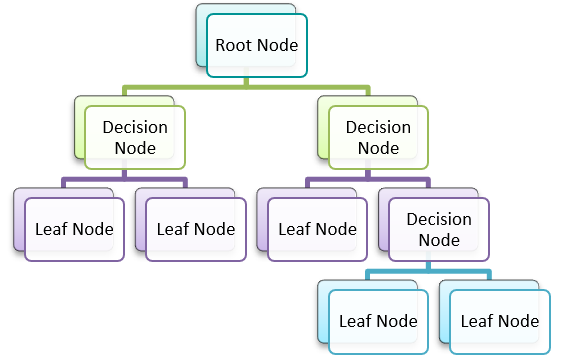
Entscheidungsbäume sind Klassifikatoren mit grafischer Darstellung als Baumstruktur, die zur Ermittlung aller möglichen Lösungen für ein bestimmtes Problem basierend auf den gegebenen Bedingungen eingesetzt werden. Entscheidungsbäume haben zwei Arten von Knoten: Entscheidungsknoten mit mehreren Verzweigungen, welche die Entscheidungsregeln darstellen, und die Blattknoten, die das Ergebnis der Entscheidungen darstellen. Die Entscheidungen werden auf der Grundlage der Merkmale des Datensatzes getroffen. Ähnlich wie bei einem Baum beginnen die Entscheidungsbäume mit dem Wurzelknoten (der eine Frage stellt) und erweitern sich dann entsprechend der Antworten auf die Fragen zu Zweigen.

**Verteilter Denial- of-Service (DDoS=Distributed DoS)**

Ein Sicherheitsangriff zur Störung des Betriebs eines Servers.

Entscheidungsbaum-Algorithmen finden in vielen Sicherheitsbereichen Anwendung, z. B. bei der Erkennung von Intrusionen und **verteilten Denial-of-Service-Angriffen (DDoS)**. Der Algorithmus kann den Netzwerkverkehr analysieren, um verdächtige Verkehrsquellen zu erkennen und somit DDoS-Verhalten aufzudecken (Al-Garadi et al., 2020).

Entscheidungsbäume



Quelle: Reza Vahidnia (2023)

#### Random Forest (RF)

Random Forest ist ein einfacher und flexibler Algorithmus für maschinelles Lernen, der Ergebnisse durch die Kombination der Ausgänge von mehreren Entscheidungsbäumen erzielt. Beim Random Forest werden mehrere Entscheidungsbäume randomisiert konstruiert und anschließend kombiniert, um ein robusteres und besseres Vorhersagemodell zu erhalten. Die Entscheidungsbäume werden darauf trainiert, eine Klasse zu wählen, und die Klasse mit den meisten Stimmen wird als endgültige Klassifizierungsausgabe verwendet.

RF-Algorithmen finden Anwendung bei der Erkennung von Intrusionen in Netzwerke, bei der Erkennung von Anomalien und bei der DDoS-Erkennung in IoT-Systemen, wobei sie mit Merkmalen aus dem Netzwerkverkehr trainiert werden. Außerdem kann RF dabei helfen, nicht autorisierte IoT-Geräte zu erkennen (Al-Garadi et al., 2020).

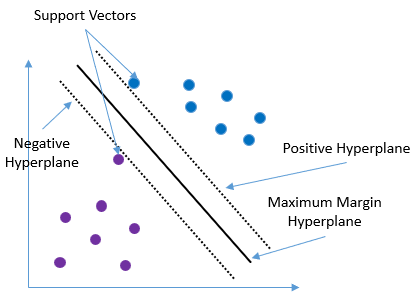
#### Logistische Regression

Die logistische Regression wird zur Vorhersage einer kategorialen abhängigen Variablen unter Verwendung einer gegebenen Gruppe von unabhängigen Parametern verwendet. Die logistische Regression ähnelt der linearen Regression mit dem Unterschied, dass anstelle einer geraden Linie eine „S“-förmige logistische Funktion (Sigmoidfunktion) angepasst wird, um die beiden Maximalwerte (d. h. 0 oder 1) vorherzusagen. Diese „S“-Kurve gibt die Wahrscheinlichkeit für ein JA oder NEIN, WAHR oder FALSCH, 1 oder 0 an.

#### Support Vector Machine (SVM)

Der Hauptzweck des SVM-Algorithmus besteht darin, die beste Linie oder Entscheidungsgrenze, die so genannte Hyperebene, zu erzeugen, die einen n-dimensionalen Raum in verschiedene Klassen unterteilen kann, so dass neue Daten in Zukunft leicht der richtigen Kategorie zugeordnet werden können. Hyperebenen werden durch die Auswahl der Extremvektoren erstellt, der so genannten Stützvektoren (Support Vectors). Der SVM-Algorithmus kann für die Klassifizierung von Bildern und Texten sowie für die Gesichtserkennung verwendet werden.

SVM-Algorithmus



Quelle: Reza Vahidnia (2023) basierend auf machine learning support vector machine algorithm (2021)

SVM-Algorithmen werden häufig in IoT-Sicherheitsanwendungen wie der Erkennung von Intrusionen und Malware eingesetzt, da diese speichereffizienten Algorithmen eine gute Option für ressourcenbeschränkte IoT-Geräte sind. SVM hat sich auch als wirksamer Algorithmus zur Absicherung intelligenter Stromnetze gegen Cyberangriffe erwiesen. Außerdem wurden SVM schon dafür benutzt, durch Knacken kryptografischer Geräte die IoT-Gerätesicherheit auszunutzen **(**Al-Garadi et al., 2020).

### Fragen zur Selbstkontrolle

1. Bitte wählen Sie den Algorithmus für maschinelles Lernen, der die beste Linie oder Entscheidungsgrenze erzeugt, die einen n-dimensionalen Raum in verschiedene Klassen unterteilen kann.

* Support Vector Machine
* Entscheidungsbäume
* Logistische Regression
* Random Forest

1. Bitte wählen Sie den Regressionsalgorithmus, bei dem die Wahrscheinlichkeiten der Werte für die Gewichte und Verzerrungen verwendet werden, um Unsicherheiten zu berücksichtigen.

* Lineare Regression
* Bayessche Lineare Regression
* Nichtlineare Regression
* Polynomische Regression

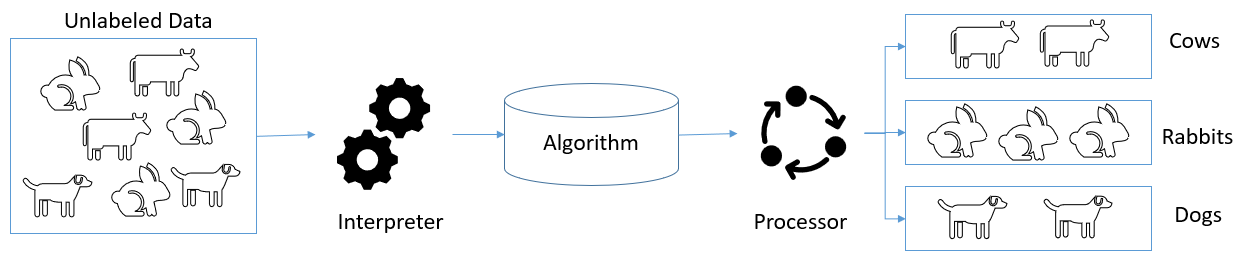
## 7.2 Unüberwachtes Lernen

Wenn es keine beschrifteten Daten für das Training eines Modells gibt, ist überwachtes Lernen nicht möglich. In solchen Fällen werden unüberwachte Algorithmen des maschinellen Lernens verwendet, um zugrunde liegende Muster und Erkenntnisse aus den gegebenen Datensätzen zu erfassen. Im Wesentlichen werden Modelle des unüberwachten Lernens anhand von unbeschrifteten Datensätzen ohne jegliche Überwachung trainiert.

Wenn beispielsweise keine beschrifteten Daten zur Klassifizierung von Dreiecks- und Vierecksbildern vorliegen, extrahiert der unüberwachte Algorithmus die Merkmale der Bilder selbst, indem er den Bilddatensatz anhand der Ähnlichkeiten zwischen den Bildern in Cluster einteilt. Im Vergleich zum überwachten Lernen wird das unüberwachte Lernen hauptsächlich für komplexere Aufgaben eingesetzt. Die Ergebnisse können jedoch weniger genau sein, da die Eingabedaten nicht beschriftet sind.

Die folgende Abbildung veranschaulicht die Funktionsweise des unüberwachten Lernens.

Unüberwachtes Lernen



Quelle: Reza Vahidnia (2023) basierend auf unsupervised machine learning (2021)

Beim unüberwachten Lernen werden zunächst die unmarkierten Daten interpretiert, um verborgene Muster zu entdecken. Anschließend werden geeignete Algorithmen angewendet, um die Daten auf der Grundlage der Ähnlichkeiten und Unterschiede zwischen den Datenobjekten in Cluster aufzuteilen.

### Algorithmen des unüberwachten Lernens

Die Algorithmen des unüberwachten Lernens lassen sich in die folgenden zwei Arten einteilen:

#### Clustering

Bei dieser Gruppierungsmethode werden die Gemeinsamkeiten zwischen den Datenobjekten analysiert, und die Objekte mit den meisten Ähnlichkeiten werden in bestimmten Clustern gruppiert.

#### Assoziation

Diese Methode wird verwendet, um Beziehungen zwischen Variablen und Elementen zu entdecken, die in großen Datenbanken zusammen auftreten. Ein typisches Beispiel für die Assoziationsmethode ist die Warenkorbanalyse, bei der ein Algorithmus feststellen kann, dass Personen, die Artikel X (z. B. einen Laptop) kaufen, häufig auch Artikel Y (z. B. ein Festplattenlaufwerk) erwerben.

Assoziationstechniken sind in der Lage, die Art eines Cyberangriffs vorherzusagen, indem sie etwaige Assoziationen zwischen den Verkehrsvariablen aufdecken. Daher werden solche Methoden verwendet, um Intrusionen zu erkennen. Im Vergleich zu anderen Algorithmen des maschinellen Lernens werden Assoziationsverfahren jedoch nur selten zur Erkennung von Sicherheitsbedrohungen in IoT-Systemen eingesetzt, da das Verhalten von Cyberkriminellen dem Verhalten legitimer Benutzender ähneln kann. Daher werden Assoziationstechniken gemeinsam mit anderen Techniken zur Bedrohungserkennung eingesetzt, um Sicherheitsbedrohungen in IoT-Umgebungen zu erkennen (**(**Al-Garadi et al., 2020).

Im Folgenden sind einige der bekanntesten Algorithmen für unüberwachtes Lernen aufgeführt:

#### K-Means Clustering

Der K-Means-Clustering-Algorithmus unterteilt einen unbeschrifteten Datensatz in K verschiedene Cluster (K ist vordefiniert), zu denen jeweils Datensätze mit ähnlichen Merkmalen gehören. Die Klassifizierung gewährleistet, dass die Summe der Abstände zwischen den Datenpunkten und ihren Clustern minimiert wird. Zu den Anwendungen von K-Means Clustering gehören die Erkennung von Intrusionen in drahtlose Sensornetzwerke (WSNs) und die Entdeckung von Sybil-Angriffen (**(**Al-Garadi et al., 2020).

#### Ausreißererkennung

Der Zweck von Ausreißererkennung (auch Anomalieerkennung genannt) besteht darin, seltene und verdächtige Datenpunkte, Elemente oder Ereignisse wie Bankbetrug oder defekte Geräte zu erkennen, die sich von anderen Datenpunkten oder Beobachtungen unterscheiden. Algorithmen zur Ausreißererkennung werden häufig eingesetzt, um Sicherheitsverletzungen in IT- und IoT-Anwendungen zu erkennen und ungewöhnliche Aktivitäten in großen Datensätzen zu entdecken.

#### Hauptkomponentenanalyse (PCA)

PCA ist ein vorhersagendes Modellierungswerkzeug und eine Technik zur Merkmalsextraktion, welche die wichtigsten Variablen in einem Datensatz erfasst und die unwichtigen weglässt. PCA transformiert die korrelierten Merkmalsbeobachtungen orthogonal in einen Satz linear unkorrelierter Merkmale, die sogenannten Hauptkomponenten. Filmempfehlungssystem, Bildverarbeitung und Optimierung der Leistungsverteilung in Kommunikationskanälen sind einige der Anwendungsgebiete von PCA. PCA wird auch für die Merkmalsauswahl verwendet, um eine Intrusion in IoT-Systeme in Echtzeit zu erkennen.

### Fragen zur Selbstkontrolle

1. Bitte nennen Sie drei Anwendungen des unüberwachten PCA-Algorithmus.

Filmempfehlungssysteme

Bildverarbeitung

Intrusionserkennung in IoT-Systemen

1. Bitte wählen Sie den Algorithmus aus, der verwendet wird, um durch Clustering der Kanalvektoren Sybil-Angreifende von normalen Sensoren zu unterscheiden.

* K-Means Clustering
* Ausreißererkennung
* Hauptkomponentenanalyse (PCA)
* Waldbaum

Zusammenfassung

Maschinelles Lernen ist eine Untergruppe der KI, bei der Trainingsdaten verwendet werden, um einen Algorithmus zu trainieren und dadurch Ergebnisse zu erzielen. Algorithmen des maschinellen Lernens haben viele Einsatzmöglichkeiten für die Sicherung von IoT-Anwendungen, bei denen die bestehenden Sicherheitsmechanismen wie Verschlüsselung, Zugangskontrolle und Authentifizierung unzureichend sind.

Beim maschinellen Lernen werden drei verschiedene Modelle verwendet, und zwar überwachtes Lernen, unüberwachtes Lernen und verstärkendes Lernen (Reinforcement Learning).

Beim überwachten maschinellen Lernen werden beschriftete Trainingsdaten als „Überwacher“ verwendet, um Maschinen so zu trainieren, dass sie die Ausgaben eines Systems für neue Daten korrekt vorhersagen können. Der Hauptzweck des überwachten maschinellen Lernens besteht darin, eine Zuordnungsfunktion zu finden, welche die Beziehung zwischen Eingabe- und Ausgabevariablen angeben kann.

Algorithmen des überwachten Lernens werden in Regression und Klassifizierung untergliedert. Sowohl Regressions- als auch Klassifizierungsalgorithmen werden mit beschrifteten Datensätzen trainiert, um Vorhersagen treffen zu können. Der Hauptunterschied zwischen ihnen besteht darin, dass Regressionsalgorithmen zur Vorhersage kontinuierlicher Werte verwendet werden, während Klassifizierungsalgorithmen zum Klassifizieren und Vorhersagen diskreter Werte dienen.

Wenn es keine beschrifteten Daten für das Training eines Modells gibt, ist überwachtes Lernen nicht möglich. In solchen Fällen werden unüberwachte Algorithmen des maschinellen Lernens verwendet, um zugrunde liegende Muster und Erkenntnisse aus den gegebenen Datensätzen zu erfassen. Die Algorithmen des unüberwachten Lernens können in Clustering- und Assoziationsmethoden eingeteilt werden. Bei der Clusteringmethode werden die Gemeinsamkeiten zwischen den Datenobjekten analysiert, und die Objekte mit den meisten Ähnlichkeiten werden in bestimmten Clustern gruppiert. Die Assoziationsmethode wird verwendet, um Beziehungen zwischen Variablen und Elementen zu entdecken, die in großen Datenbanken zusammen auftreten.