Lerneinheit

[Internet der Dinge]

Projekt: B-SAFE
Nummer: 2018-1CZ01-KA204-048148

Funded by the
Erasmus+ Programme
of the European Union

Co-funded by the
Erasmus+ Programme
of the European Union

Internet der Dinge

Einführung

Das Internet der Dinge, allgemein bekannt als IoT (Internet of Things), ist Teil der vierten industriellen Revolution, nämlich Industrial 4.0, und hat eine direktere Auswirkung auf den Einzelnen als Endbenutzer.

Das IoT ist ein System miteinander verbundener Computergeräte, mechanischer und digitaler Maschinen, Objekte, Tiere oder Menschen, das in der Lage ist, Daten über ein Netzwerk zu übertragen, ohne dass eine Interaktion von Mensch zu Mensch oder von Mensch zu Computer erforderlich ist. Das erste "offizielle" IoT-Gerät war ein Cola-Automat auf dem Campus der Carnegie Mellon University in Pittsburgh, Pennsylvania, im Jahr 1982. Die Studenten wollten im Voraus wissen, ob neu geladene Dosen Soda auf dem Höhepunkt der Kälte waren, und so rüsteten sie den Automaten so aus, dass sie diese Information an einen Computer in einem nahe gelegenen Büro melden konnten.

Trotz ihres Alters entwickelt sich die IoT-Technologie ständig weiter, so dass wir mit störenden Veränderungen im Zusammenhang mit unseren Lebensgewohnheiten konfrontiert sind, da es unzählige Möglichkeiten und Anwendungen des IoT sowohl in der Industrie als auch im täglichen Leben gibt.

Es bietet zwar effektive und effiziente Lösungen für zu viele Probleme der realen Welt, aber es gibt bedeutende Herausforderungen in Bezug auf Sicherheit und Privatsphäre, die nicht ignoriert werden dürfen.

Praktische Relevanz - Hierfür benötigen Sie das Wissen und die Fähigkeiten

Nach dem Erlernen dieser Inhaltseinheit werden Sie wissen, was das Internet der Dinge ist und was die Hauptanwendungen dieser neuen Technologie sind.

Darüber hinaus werden Sie über die häufigsten Probleme im Zusammenhang mit der Sicherheit und dem Datenschutz im Internet der Dinge informiert und erfahren, wie Sie im Falle eines Cyberangriffs auf eines Ihrer intelligenten Geräte reagieren sollten.

Co-funded by the
Erasmus+ Programme
of the European Union

1.Wissen aufbauen - Internet der Dinge im Alltag

Im Laufe der Jahre gab es im Bereich des Internet der Dinge (Internet of Things, IoT) sowohl in technologischer Hinsicht als auch in Bezug auf das Marktwachstum ein rasantes Wachstum. Die Vernetzung von Computern, die als "Internet" bezeichnet wird, revolutionierte die Art und Weise, wie wir Informationen austauschen. Das IoT kann als nächste Revolution in der Art und Weise angesehen werden, wie wir die Informationen wahrnehmen und teilen (Virat, 2018). Im Kasten unten finden Sie eine vereinfachte Definition des IoT:

Definition

Internet der Dinge ist das Konzept, jedes Gerät (sofern es über einen Ein-/Aus-Schalter verfügt) mit dem Internet und anderen angeschlossenen Geräten zu verbinden. Das IoT ist ein **riesiges Netzwerk miteinander verbundener Dinge und Menschen** - alle sammeln und teilen Daten über die Art und Weise, wie sie benutzt werden, und über die Umwelt um sie herum.

Geräte und Objekte mit eingebauten Sensoren sind mit einer Plattform für das Internet der Dinge verbunden, die Daten von den verschiedenen Geräten integriert und Analysen anwendet, um die wertvollsten Informationen mit Anwendungen zu teilen, die für spezifische Bedürfnisse entwickelt wurden. In der Abbildung unten finden Sie zwei gute Beispiele für eine IoT-Technologie.

Wie wir bereits gesehen haben, ist das IoT ein weit gefasster Begriff, der sich auf das riesige Netzwerk von Geräten bezieht, die mit dem Internet verbunden sind und heute existieren.

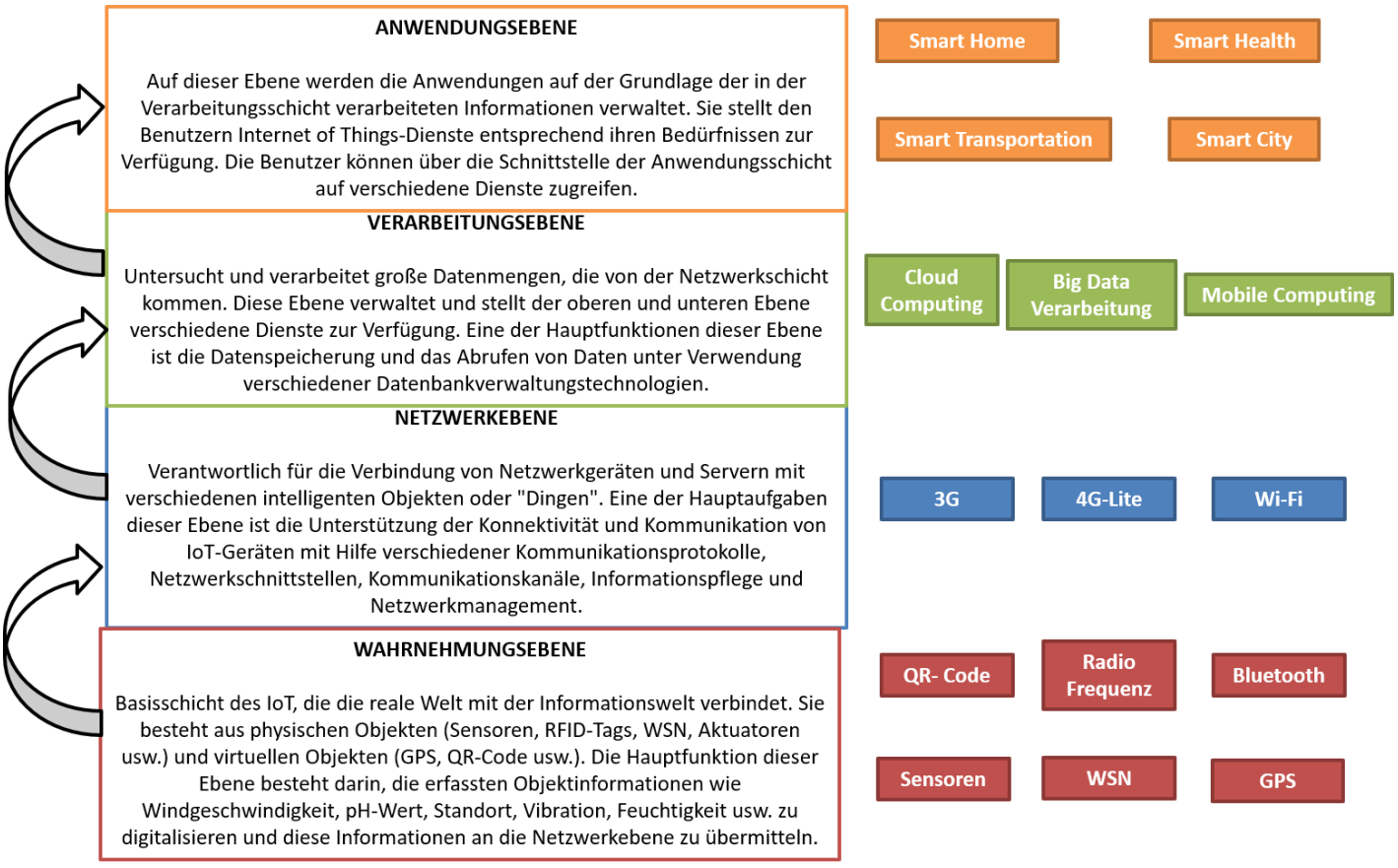
Co-funded by the
Erasmus+ Programme
of the European Union

Das Internet der Dinge verspricht die wichtigste technologische Entwicklung für Verbraucher seit dem Aufkommen des Smartphones zu werden. ExpertInnen gehen davon aus, dass diese Technologie schließlich bis 2021 einen Jahresumsatz von mehr als 123 Milliarden Dollar generieren wird, und die Statistiken weisen darauf hin, dass bis Ende 2020 mehr als 36 Milliarden Geräte an das Internet angeschlossen sein werden.

Tatsächlich arbeiten große Unternehmen wie Amazon, Google und Tesla bereits mit Software-Entwicklungsdiensten, um hochmoderne IoT-Geräte herzustellen. Es wird erwartet, dass das IoT fortgeschrittene intelligente Häuser zur Realität werden lässt. Weitere Beispiele für IoT-Technologien sind **selbstfahrende Autos, tragbare Geräte, die Körpermarkierungen verfolgen, das Einhalten von Verhaltensänderungen durch den Patienten bzw. die Patientin, SprachassistentInnen (z.B. Alexa), intelligente Heizsysteme usw.**

Deshalb können wir leicht erkennen, dass die gesamte Gesellschaft zu einem bestimmten Zeitpunkt mit einem IoT-Gerät in Berührung kommt. Daher ist es sehr **wichtig, das allgemeine Verhalten** der BürgerInnen und ihre Privatsphäre/Sicherheit zu verbessern.

Die Dynamik, Intelligenz und Mobilität des IoT machen es zu einer Technologie mit hoher Nachfrage, machen das IoT aber auch unter **Sicherheits- und Datenschutzbedingungen verwundbar und riskant**. Um die Komplexität dieser Herausforderung zu verstehen, muss man die grundlegende Architektur des IoT verstehen, die durch eine **dynamische Struktur** gekennzeichnet ist. Die Anzahl der Schichten, aus denen sich die Architektur des IoT zusammensetzt, ist von ExpertIn zu ExpertIn sehr unterschiedlich, aber alle sind sich einig, dass das IoT aus mindestens vier Schichten besteht: **Wahrnehmung (Perception Layer), Netzwerk (Network Layer), Verarbeitung (Processing Layer) und Anwendung (Application Layer)**.



Wie Sie feststellen können, erleichtert die Anwendungsschicht die globale Verwaltung der intelligenten Anwendungen und bietet dem Nutzendem spezifische Dienste an. In der nächsten Tabelle sind die Top-Anwendungen des IoT im täglichen Leben

Smart Home Es ist ein vernetztes Zuhause, in dem alle Arten von Dingen über das Internet miteinander interagieren. In einem Smart Home können Sie beispielsweise die Klimaanlage auf dem Heimweg einschalten oder die Waschmaschine aktivieren, während Sie bei der Arbeit sind. Im Wesentlichen ist alles miteinander vernetzt, um Ihr Leben einfacher und bequemer zu machen.

Smart Home	Es ist ein vernetztes Zuhause, in dem alle Arten von Dingen über das Internet miteinander interagieren. In einem Smart Home können Sie beispielsweise die Klimaanlage auf dem Heimweg einschalten oder die Waschmaschine aktivieren, während Sie bei der Arbeit sind. Im Wesentlichen ist alles miteinander vernetzt, um Ihr Leben einfacher und bequemer zu machen.
Wearable	Diese Geräte (wie z.B. Fit Bit) sammeln Daten und Informationen über den Nutzenden, die später vorverarbeitet werden, um wesentliche Erkenntnisse zu gewinnen. Diese kleinen, hocheffizienten Geräte decken die Anforderungen an Fitness, Gesundheit und Unterhaltung weitgehend ab.
Smart/Connected Cars	Ein intelligentes Fahrzeug, das in der Lage ist, seinen eigenen Betrieb, die Wartung sowie den Komfort der Passagiere zu optimieren. Diese Fahrzeuge werden im intelligenten Transport eingesetzt - das schließt Wasserstraßen, Eisenbahnen, Straßen usw. ein. - Sie erhalten Echtzeit-Informationen über Straßen, Unfälle, Umleitungen und Sperrungen in einer Weise, die dem Fahrenden und den Fahrgästen ein Höchstmaß an Sicherheit bietet.
Smart Cities	Sie umfasst alles, was eine Stadt ausmacht, wie Überwachung, Transport, Energiemanagementsysteme, Wasserverteilung, städtische Sicherheit und Umweltüberwachung. Beispielsweise kann die Regierung automatisch über gemessene Verschmutzungswerte oder Energieknappheit usw. informiert werden.
Smart Agriculture	Die LandwirtInnen nutzen aussagekräftige Erkenntnisse aus den Daten, um eine bessere Investitionsrendite zu erzielen. Die Messung von Bodenfeuchtigkeit und Nährstoffen, die Kontrolle des Wasserverbrauchs für das Pflanzenwachstum und die Bestimmung von kundenspezifischen Düngemitteln sind einige einfache Anwendungen des IoT.
Energieverwaltung	Die Stromnetze der Zukunft werden nicht nur intelligent genug, sondern auch höchst zuverlässig

	sein. In intelligenten Stromnetzen trägt der Einsatz von intelligenten Zählern, Home-Gateways, intelligenten Steckern und angeschlossenen Geräten dazu bei, Ressourcen zu schonen und Geld für Verbraucher, Hersteller und Versorger zu sparen.
Smart Healthcare	Ein vernetztes Gesundheitssystem und intelligente medizinische Geräte stellen eine Revolution für die Gesellschaft dar, da sie nicht nur für Unternehmen, sondern auch für das Wohlergehen der Menschen im Allgemeinen erhebliche Auswirkungen haben. Die Anwendung des IoT im Gesundheitsbereich umfasst die Gewinnung von Informationen über Gesundheitsparameter eines Individuums wie Blutdruck, Körpertemperatur, Herzschlagmessungen usw. durch extrem stromsparende, hoch energieeffiziente und kleine tragbare Geräte. Diese gesammelten Informationen können an die jeweiligen Personen und Gesundheitszentren für weitere Maßnahmen der Ärzte weitergegeben werden.

1.Wissen anwenden

Übung SINGLE CHOICE

Situation: Was ist das "Internet der Dinge"?
Aufgabe: Bitte bestimmen Sie die richtige Option nach dem Single-Choice-Prinzip: Nur eine Antwort ist richtig.

- IoT ist ein Netzwerk von verbundenen Servern, auf die über das Internet zugegriffen wird.
- IoT ist die Digitalisierung und Automatisierung jedes Teils des Unternehmens sowie des Herstellungsprozesses.
- IoT ist ein globales Weitverkehrsnetz, das Computersysteme auf der ganzen Welt miteinander verbindet.
- IoT ist eine beginnende Technologie, die sich auf die Verbindung von Dingen oder Geräten untereinander und mit Menschen oder Benutzern konzentriert, um einige gemeinsame Ziele zu erreichen.

Übung MULTIPLE CHOICE

Situation: Was sind die Hauptanwendungen des Internet der Dinge?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip aus. Keine, eine, mehr als eine oder alle Optionen können wahr sein

- Überwachung von Stromleitungen und Übergang zu intelligenten Stromnetzen.
- Management der Produktionslieferkette im Einzelhandel.
- Produktionslieferkettenmanagement in der verarbeitenden Industrie.
- Regulierung von Wasser in der Landwirtschaft.

Co-funded by the
Erasmus+ Programme
of the European Union

2.Wissen aufbauen - Internet der Dinge und Fragen der Sicherheit und des Datenschutzes

Intelligente Verbrauchergeräte, die mit dem Internet der Dinge verbunden sind, sammeln ständig persönliche Informationen von VerbraucherInnen. Daher ist eine der größten Sorgen im Zusammenhang mit der Umsetzung des Internet der Dinge in unserem täglichen Leben mit der Sicherheit und dem Schutz persönlicher und sogar sensibler persönlicher Daten verbunden, da der Diebstahl persönlicher Daten Einzelpersonen, Unternehmen und der Gesellschaft insgesamt schweren Schaden zufügen kann. Das Internet der Dinge ist eine allgegenwärtige Technologie mit einer komplexen Architektur und Struktur. Folglich schafft sie neuartige Sicherheits- und Datenschutzprobleme, die bisher als harmlos oder undefiniert galten. Diese Bedenken beziehen sich hauptsächlich auf:

1. **IoT-Technologien** haben im Vergleich zu Smartphones und Desktop-Computern **eine längere Lebensdauer**.
2. Es gibt eine **Vielzahl von HerstellerInnen**, von denen die meisten kein traditionelles Fachwissen im Bereich der Informationstechnologie (IT) besitzen, was zu Interoperabilitätsproblemen und mangelnder Sicherheitshygiene führt.
3. Dieser **Mangel an IT-Fachwissen** erstreckt sich auch auf die Endbenutzer (die de facto alle Systemadministratoren sind).
4. Die Anzahl der Geräte und die globale Vernetzung verschlimmern alle Probleme. Tatsächlich wird geschätzt, dass es derzeit 50 Milliarden angeschlossene Geräte gibt.

Die Sicherheit von Daten und die Privatsphäre der NutzerInnen sind verschiedene Konzepte, die sich jedoch nicht gegenseitig ausschließen. Tatsächlich gefährdet ein Sicherheitsangriff oder Cyberattack automatisch die Privatsphäre des Benutzers.
Die Herausforderungen, die bewältigt werden müssen, um IoT-Sicherheits- und Datenschutzprobleme zu lösen, sind immens. Dies liegt in erster Linie an den vielen Einschränkungen, die mit der Bereitstellung von Sicherheit und Privatsphäre in IoT-Systemen verbunden sind. Dennoch wird im nachfolgenden Kasten eine kurze Definition dieser Konzepte, angewandt auf das IoT, vorgestellt.

Die Art der Bedrohungen und Angriffe auf die Sicherheit und Privatsphäre, denen das IoT ausgesetzt ist, hängt von seinen Schichten ab, da jede Schicht unterschiedliche Besonderheiten und damit verbundene Technologien aufweist. In der folgenden Tabelle wird eine Zusammenfassung der häufigsten Cyberangriffe auf den IoT-Rahmen sowie der Grad der Auswirkungen auf die vier Schichten, aus denen sich die IoT-Architektur zusammensetzt, dargestellt:

	Kurzbeschreibung	WAHRNEHMUNGSSCHICHT	NETZWERKER	VERARBEITUNGSSCHICHT	ANWENDUNGSSCHICHT
Schädlicher Code	Jeder Code in irgendeinem Teil eines Softwaresystems oder Skripts, der unerwünschte Auswirkungen, Sicherheitsverletzungen oder Schäden an einem System verursachen soll	Hoch	Hoch	Niedrig	Hoch
DoS-Angriff	Cyberattack, bei dem der Täter bzw. die Täterin versucht, einen Rechner oder eine Netzwerkressource unzugänglich zu machen	Niedrig	Hoch	Hoch	Niedrig

Routing-Informationen	Protokolle, die Router zum Austausch von Netzwerktopologie-Informationen verwenden können	Niedrig	Hoch	Hoch	Niedrig
Lauschangriff	Ist der Akt des heimlichen oder heimlichen Mithörens von privaten Gesprächen oder Kommunikationen anderer ohne deren Zustimmung	Hoch	Medium	Hoch	Medium
Identitätsdiebstahl	Absichtliche Verwendung der Identität einer anderen Person, gewöhnlich als Methode zur Erlangung eines finanziellen Vorteils oder anderer persönlicher Informationen	Hoch	Medium	Hoch	Medium
Sinkhole-Angriff	Bedroht die Sicherheit von WSNs auf fast allen Ebenen ihres Protokollstapels	Medium	Hoch	Niedrig	Niedrig
Phishing-Angriff	Betrügerischer Versuch, an vertrauliche Informationen oder Daten zu gelangen, wird typischerweise durch E-Mail-Spoofing oder Instant Messaging durchgeführt	Niedrig	Niedrig	Medium	Hoch

Wie Sie beobachten können, gibt es eine Vielzahl möglicher Angriffe, die die Sicherheit und Privatsphäre von IoT-Geräten gefährden können, wobei die Auswirkungen je nach Schicht unterschiedlich stark sind. Daher gibt es beträchtliche Herausforderungen, die von allen beteiligten Parteien bewältigt werden müssen: Hersteller oder Entwickler von IoT-Geräten, Regierung und Endbenutzer.

2.Wissen anwenden

Übung MULTIPLE CHOICE

Situation: Welche Aussagen sind in Bezug auf die Sicherheit von IoT-Geräten und ihren Nutzenden wahr?

Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip aus. Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Datensicherheit ist erforderlich, wenn Daten erzeugt und gespeichert werden.
- Sicherheitsanforderungen für IoT-Anwendungen müssen in drei Schichten angewendet werden: Anwendungsschicht, Netzwerkschicht und Wahrnehmungsschicht.
- Die Wahrscheinlichkeit des Auftretens eines Phishing-Angriffs in einem IoT-Gerät ist in seiner Verarbeitungsschicht höher.
- Die Architektur des IoT erlaubt es böswilligen Entitäten, Schwachstellen auszunutzen, die jeder der IoT-Schichten inhärent sind.
- Ein bösartiger Code kann mindestens drei Schichten betreffen.

Übung SINGLE CHOICE

Situation: Welche Aussage trifft unter Berücksichtigung der Privatsphäre der IoT-Nutzenden zu?
Aufgabe: Bitte bestimmen Sie die richtige Option nach dem Single-Choice-Prinzip: Nur eine Antwort ist wahr.

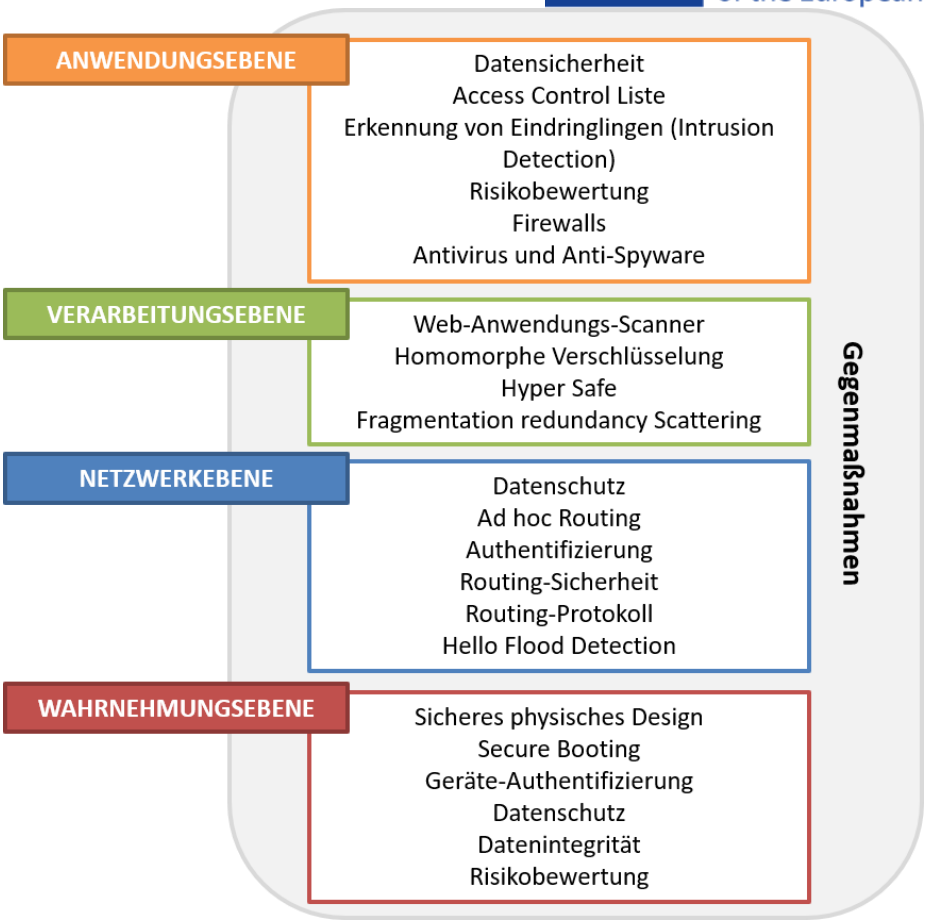
- Das signifikante Wachstum, das das IoT in den letzten Jahren gezeigt hat, hat mehrere Bedenken hinsichtlich der Privatsphäre mit sich gebracht, da die Datenverfügbarkeit abnimmt, was durch gemeinsame und übliche Eigenschaften des IoT gefördert wird.
- Die HerstellerInnen müssen den Schutz der persönlichen Daten der Nutzenden im Zusammenhang mit ihren Bewegungen, Gewohnheiten und Interaktionen gewährleisten.
- Die Privatsphäre bezieht sich darauf, wie gut sich die IoT-Geräte gegen den Diebstahl von Benutzerdaten schützen.
- Die Privatsphäre ist nur in der Anwendungsschicht gefährdet.

3.Wissen aufbauen - Internet der Dinge und Schutz seiner BenutzerInnen

Anfang des Jahres 2019 gelang es CNN, über eine Suchmaschine für IoT-Geräte Shodan auf eine Vielzahl von Kamerafeeds zuzugreifen. Sie beobachteten aus der Ferne Kinder, die in einer Turnhalle der Mittelschule in Indonesien spielten, einen Mann, der sich in einer Moskauer Wohnung bettfertigte, eine australische Familie, die aus ihrer Garage kam und ging, und eine Frau, die in Japan ihre Katze fütterte. Allen schien nicht bewusst zu sein, dass sie ihr Leben in jeder Sekunde des Tages online übertragen. Laut CNN hatte keine der Kameras Sicherheitskontrollen durchlaufen und stand jedem offen, der die richtige Adresse kannte.

Um zu vermeiden, dass Ihnen eine solche Situation passiert, gibt es einige Techniken, Verfahren und Verhaltensweisen, die sowohl vom Entwickler des IoT-Geräts als auch vom Nutzenden des intelligenten Geräts übernommen werden sollten. Unten sehen Sie einige Maßnahmen, um zu reagieren und Cyberattacken in allen Schichten, aus denen IoT-Geräte bestehen, zu verhindern.

Co-funded by the
Erasmus+ Programme
of the European Union



Wie Sie beobachten können, sollten die meisten der Datenschutz- und Sicherheitsmechanismen für das Internet der Dinge implementiert werden. IoT-Entwickler sollten ihre Bemühungen auf die Schaffung von Geräten konzentrieren, die physisch gesichert und mit kryptographischen Algorithmen, gehärteten Gateway-Plattformen, komplexer Verschlüsselung, Anti-Virus, Anti-Spyware, Anti-Adware und fortschrittlichen und aktualisierten Sicherheitstechniken geschützt sind. Daher kann sich der Nutzende auf den Sicherheitsmechanismus verlassen, der bereits in den IoT-Geräten integriert ist, um seine Privatsphäre und Sicherheit zu schützen. Nichtsdestotrotz gibt es einige Maßnahmen, die Sie als IoT-Verbraucher bzw. Verbraucherin kennen müssen, um verschiedene IoT-Sicherheits- und Datenschutzbedrohungen zu überwinden:

1. - Lesen Sie die Sicherheitsanforderungen und die Datenschutzrichtlinie für die Geräte

Wählen Sie immer ein IOT-Gerät von einem vertrauenswürdigen und transparenten Herstellendem. Sie sind berechtigt, die im IoT implementierte Sicherheitstechnik zu kennen.
Ebenso sollten Sie immer die Datenschutzerklärung des Geräts lesen, da Sie sich darüber im Klaren sein müssen, wie Ihr IoT-Gerät funktioniert und aus welchen Gründen Ihre Daten von IoT-Smart-Geräten gesammelt und verwendet werden. Einfach ausgedrückt: Bevor Sie ein IoT-Gerät benutzen, sollten Sie wissen, ob Sie dazu in der Lage sind:
1) Auf die von Ihnen via IoT gesammelten Daten zugreifen, sie einsehen und entfernen können;
2) die Verbindung zu Ihren IoT-Geräten trennen, wenn Sie dies wünschen;
3) der Speicherung Ihrer persönlichen Daten auf dem IoT-Gerät zustimmen.

2. - Hören Sie auf, das Standardpasswort zu verwenden!

Das erste, was Sie mit Ihrem IoT-Gerät tun sollten, ist zu prüfen, ob es Ihnen erlaubt, die Standardpasswörter zu ändern. Verwenden Sie immer ein sicheres, eindeutiges Passwort für jedes einzelne Gerät, das Sie besitzen. Vergessen Sie nicht, auch die Passwörter Ihres Wi-Fi-Routers zu ändern!

Co-funded by the
Erasmus+ Programme
of the European Union

3. - Deaktivieren Sie den Fernzugriff (WAN) auf das Gerät

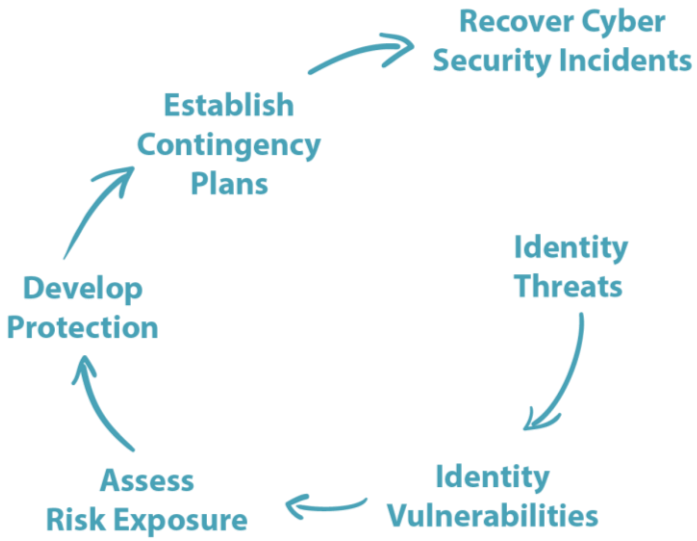
Wenn Sie gerade zu Hause sind, googeln Sie "Was ist meine IP-Adresse" auf Ihrem Computer. Was Sie dort sehen, ist Ihre WAN-IP-Adresse. Diese Adresse ist im Internet zu jedem Zeitpunkt eindeutig. Wenn Sie auf Reisen gehen, können Sie diese IP-Adresse für den Fernzugriff auf Ihre Smart-Home-Geräte verwenden. Wenn die Geräte nicht gesichert sind, ist die IP-Adresse alles, was für jeden, der darauf zugreifen möchte, notwendig ist. Tatsächlich war es genau das, was CNN für den Zugriff auf eine Vielzahl von Kamerafeeds verwendete!

4. - Deaktivieren Sie die Funktionen, die nicht verwendet werden

Ein vertrauenswürdiges intelligentes Gerät ist ein Gerät, das es Ihnen erlaubt, seine Funktionen zu personalisieren. Wenn Sie z.B. Ihre Smart-Uhr nicht zur Erfassung Ihrer letzten Trainingsdaten verwenden, aktivieren Sie die Bluetooth-Verbindung; oder wenn Sie Ihren Joggingpfad nicht aufzeichnen müssen, aktivieren Sie das GPS und den Positionstrack.

5. - Seien Sie ein Super-Agent bzw. eine Super-Agentin der Cybersicherheit!

Wussten Sie, dass 95 % der Verstöße gegen die Cybersicherheit auf menschliches Versagen zurückzuführen sind? Daher sind Kenntnisse im Bereich der Cybersicherheit der wichtigste Weg, um Cyberangriffe zu verhindern. Um ein Super-Agent bzw. eine Super-Agentin der Cybersicherheit zu sein, müssen Sie alle Phasen des Cyber-Sensibilisierungsplans beherrschen:



Unabhängig davon, ob Sie die Geräte des Internet der Dinge in Ihrem täglichen Leben nutzen oder ob Sie ein Geschäftsinhaber bzw. eine Geschäftsinhaberin oder ManagerIn sind, der die Technologie und das Internet bei seinen täglichen Aktivitäten einsetzt, müssen Sie die Chancen erhöhen, einen Sicherheits- oder Datenschutzangriff abzufangen, bevor er vollständig in Kraft tritt, um den Schaden zu minimieren und die Kosten für die Wiederherstellung zu senken.

Inzwischen verfügen Sie über alle Grundkenntnisse, um bei der Identifizierung von Bedrohungen und Schwachstellen, bei der Risikobewertung und beim Schutz des Geräts ein Ass zu sein. Was aber, wenn Sie trotz aller Vorbeugung und Sorgfalt immer noch Opfer eines Cyberangriffs werden, während Sie das Internet der Dinge nutzen? Die Antwort beruht auf den 4 W's: Wer, Was, Wann und Welche.

WER

Machen Sie eine Liste, wen Sie im Falle einer beginnenden Delle anrufen können. Es ist von entscheidender Bedeutung, dass Sie wissen, wer die Entscheidung zur Einleitung von Einziehungsverfahren trifft

und wer der primäre Ansprechpartner für die zuständigen Mitarbeiter der Strafverfolgungsbehörden ist.

WAS

Stellen Sie sicher, dass Sie einen Plan haben, was im Falle eines Vorfalls mit Ihren Daten zu tun ist. Dazu kann das Herunterfahren und Neustarten Ihrer gesamten IoT-Systeme gehören.

WANN

Bestimmen Sie, wann Notfallpersonal, CybersicherheitsexpertInnen, Dienstleistungs- oder VersicherungsanbieterInnen alarmiert werden sollen.

WELCHE

Ihr Reaktionsplan sollte die Arten von Aktivitäten klären, die einen Vorfall der Informationssicherheit darstellen. In Bezug auf eine Organisation gehören dazu Vorfälle wie der Ausfall Ihrer Website für mehr als eine bestimmte Zeitspanne oder Beweise für Informationsdiebstahl.

Vergessen Sie nicht, Ihre Familie, Freunde und/oder MitarbeiterInnen in den Cyber-Sensibilisierungsplan einzubeziehen, da **jeder IoT-Benutzer für die Cybersicherheit verantwortlich** ist!

3.Wissen anwenden

Übung MULTIPLE CHOICE

Situation: Welche Sicherheitsmaßnahmen sollten Sie ergreifen, um Cyberattacken auf Ihre IoT-Geräte zu verhindern?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip aus. Keine, eine, mehr als eine oder alle Optionen können wahr sein

- Homomorphe Verschlüsselung installieren.
- Installieren Sie Firewalls.
- Fragmentierungsredundanzstreuung schaffen.
- Standardpasswörter des Routers ändern.
- Deaktivieren Sie nicht genutzte Funktionen in meinem intelligenten Gerät.
- Deaktivieren Sie den Fernzugriff auf das Smart-Gerät.

Übung MULTIPLE CHOICE

Situation: Was sollten Sie tun, um ein Superagent der Cybersicherheit zu werden?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip aus. Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Lernen Sie, wie man programmiert, um IoT-Geräte zu verschlüsseln.
- Einen Kontingentplan nach den 4 W's aufstellen: "Was wird erzeugt?", "Wo werden Daten gespeichert?", "Wann werden Daten verwendet?" und "Mit wem werden Daten geteilt?
- Richten Sie einen Kontingentplan im Anschluss an die 4 W's ein: "Wen soll ich anrufen?" "Wie gehe ich vor?", "Wann sollen andere alarmiert werden?" und "Welche Aktivitäten sind Vorfälle?
- Beziehen Sie meine ganze Familie, Gleichaltrige und MitarbeiterInnen in das Bewusstsein für Cybersicherheit ein.
- Entwickeln Sie den Plan für die Reaktion auf Vorfälle erst nach einer Sicherheitsverletzung, denn nur so können Sie die richtigen Maßnahmen für die noch bevorstehenden Vorfälle kennen.

Co-funded by the
Erasmus+ Programme
of the European Union

Quellen

Analytics Vidhya (August 26, 2016). *10 Real World Applications of Internet of Things (IoT) – Explained in Videos.* Retrievd from https://www.analyticsvidhya.com/blog/2016/08/10-youtube-videos-explaining-the-real-world-applications-of-internet-of-things-iot/

Clark, J. (November 17, 2016*). What is the Internet of Things (IoT)?* Retrieved from https://www.ibm.com/blogs/internet-of-things/what-is-the-iot/

Evans, D. (2011). *The internet of things how the next evolution of the internet is changing everything.* Cisco White Paper, 1–11. Retrieved from

https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

Griffiths, J. (February 2, 2019). *'Internet of things' or 'vulnerability of everything'? Japan will hack its own citizens to find out.* Retrived from https://edition.cnn.com/2019/02/01/asia/japan-hacking-cyber-security-iot-intl

Kelbert, J. (September 24, 2019). *5 Interesting Facts About the IoT.* Retrieved from https://blog.flexis.com/5-interesting-facts-about-the-internet-of-things-iot

Mena, D. M., Papapanagiotou, I. and Yang, B. (2018) *Internet of things: Survey on security.* Information Security Journal: A Global Perspective, 27:3, 162-182, DOI: 10.1080/19393555.2018.1458258

Finance Monthly (September 5, 2019). *The Worst And Weirdest IoT Hacks Of All Times.* Retrived from https://www.finance-monthly.com/2019/09/the-worst-and-weirdest-iot-hacks-of-all-times/

Ngo, D. (December 22, 2015). *Home networking explained, part 9: Access your home computer remotely.* Retrieved from https://www.cnet.com/how-to/home-networking-explained-part-9-access-your-home-computer-remotely/

Oorschot, P. C and Smoth, S. W. (2019). *The Internet of Things: Security Challenges.* IEEE Security and Privacy Magazine, 17(5):7-9. DOI: 10.1109/MSEC.2019.2925918

Spencer, T. (August 8, 2019). *How to Respond to a Cyber Attack.* Retrived from https://www.industryweek.com/sponsored/article/22028042/how-to-respond-to-a-cyber-attack

Viriat, M. S. et al. (2018). *Security and Privacy Challenges in Internet ofn Things*. Proceedings of the 2nd International Conference on Trends in Electronics and Informatics. IEEE Conference Record: # 42666; IEEE Xplore ISBN:978-1-5386-3570-4

Co-funded by the
Erasmus+ Programme
of the European Union

Wissen sichern

Internet der Dinge, oder einfach IoT, ist heutzutage ein Schlagwort. Das IoT wird zweifelsohne die Art und Weise verändern, wie der Einzelne mit der Welt und der Technologie um ihn herum interagiert. Dieses **Netzwerk** von Geräten, die mit **dem Internet verbunden** sind, wird viele positive Auswirkungen haben.

Das Internet der Dinge stellt eine Revolution in der Art und Weise dar, wie wir miteinander interagieren. Tatsächlich hat das IoT neue Arten der Interaktion geschaffen, da es eine **Technologie ist, die die Verbindung zwischen Dingen, Prozessen, Menschen, Tieren und fast allem, was wir um uns herum sehen, über das Internet ermöglicht.**

Obwohl es sich um ein einfaches Konzept handelt, braucht das IoT eine ausgeklügelte Architektur, um richtig zu funktionieren. Die IoT-Architektur besteht aus mindestens **vier Schichten**, nämlich der Wahrnehmungsschicht, der Netzwerkschicht, der Verarbeitungsschicht und der Anwendungsschicht. In dieser letzten Schicht haben wir die Wahrnehmung des Nutzens des IoT, da sie intelligente Anwendungen und intelligente Geräte darstellt, die in vielen Bereichen eingesetzt werden könnten und sie "intelligenter" machen: intelligente Häuser, intelligente Landwirtschaft, intelligente Städte, intelligente Gesundheitsfürsorge und viele andere.

Die Dynamik, Intelligenz und Mobilität des IoT machen es zu einer Technologie mit hoher Nachfrage, aber es macht **das IoT auch unter Sicherheits- und Datenschutzbedingungen verwundbar und riskant**. Alle Schichten des IoT sind verschiedenen Cyberattacken ausgesetzt. Daher müssen sich die **EntwicklerInnen intelligenter Geräte aktiv an der Entwicklung wirksamer Sicherheits- und Datenschutzmaßnahmen** beteiligen, um das IoT in Bezug auf Sicherheit robuster zu machen.

Nichtsdestotrotz ist die Hauptursache für die Verwundbarkeit des IoT das **mangelnde Sicherheitsbewusstsein**. Menschen, Unternehmen und die Gesellschaft insgesamt müssen sich für die **Verbesserung der Cybersicherheitskompetenz einsetzen**, um die Hauptursache für Cybersicherheitsverletzungen zu beseitigen: menschliches Versagen.

Denken Sie immer daran, seien Sie ein Superagent bzw. eine Superagentin der Cybersicherheit!

Co-funded by the
Erasmus+ Programme
of the European Union

Lösungsschlüssel
(die korrekten Antworten sind fett markiert)

1.Wissen anwenden

Situation: Was ist das "Internet der Dinge"?
Aufgabe: Bitte bestimmen Sie die richtige Option nach dem Single-Choice-Prinzip: Nur eine Antwort ist richtig.

- IoT ist ein Netzwerk von verbundenen Servern, auf die über das Internet zugegriffen wird.
- IoT ist die Digitalisierung und Automatisierung jedes Teils des Unternehmens sowie des Herstellungsprozesses.
- IoT ist ein globales Weitverkehrsnetz, das Computersysteme auf der ganzen Welt miteinander verbindet.
- **IoT ist eine beginnende Technologie, die sich auf die Verbindung von Dingen oder Geräten untereinander und mit Menschen oder Benutzern konzentriert, um einige gemeinsame Ziele zu erreichen.**

Situation: Was sind die Hauptanwendungen des Internet der Dinge?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip aus. Keine, eine, mehr als eine oder alle Optionen können wahr sein

- **Überwachung von Stromleitungen und Übergang zu intelligenten Stromnetzen.**
- **Management der Produktionslieferkette im Einzelhandel.**
- **Produktionslieferkettenmanagement in der verarbeitenden Industrie.**
- **Regulierung von Wasser in der Landwirtschaft.**

2.Wissen anwenden

Situation: Welche Aussagen sind in Bezug auf die Sicherheit von IoT-Geräten und ihren Nutzenden wahr?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip aus. Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- **Datensicherheit ist erforderlich, wenn Daten erzeugt und gespeichert werden**.
- Sicherheitsanforderungen für IoT-Anwendungen müssen in drei Schichten angewendet werden: Anwendungsschicht, Netzwerkschicht und Wahrnehmungsschicht.
- Die Wahrscheinlichkeit des Auftretens eines Phishing-Angriffs in einem IoT-Gerät ist in seiner Verarbeitungsschicht höher.
- **Die Architektur des IoT erlaubt es böswilligen Entitäten, Schwachstellen auszunutzen, die jeder der IoT-Schichten inhärent sind.**
- **Ein bösartiger Code kann mindestens drei Schichten betreffen.**

Situation: Welche Aussage trifft unter Berücksichtigung der Privatsphäre der IoT-Nutzenden zu?
Aufgabe: Bitte bestimmen Sie die richtige Option nach dem Single-Choice-Prinzip: Nur eine Antwort ist wahr.

- Das signifikante Wachstum, das das IoT in den letzten Jahren gezeigt hat, hat mehrere Bedenken hinsichtlich der Privatsphäre mit sich gebracht, da die Datenverfügbarkeit abnimmt, was durch gemeinsame und übliche Eigenschaften des IoT gefördert wird.

- **Die HerstellerInnen müssen den Schutz der persönlichen Daten der Nutzenden im Zusammenhang mit ihren Bewegungen, Gewohnheiten und Interaktionen gewährleisten.**
- Die Privatsphäre bezieht sich darauf, wie gut sich die IoT-Geräte gegen den Diebstahl von Benutzerdaten schützen.
- Die Privatsphäre ist nur in der Anwendungsschicht gefährdet.

3.Wissen anwenden

Situation: Welche Sicherheitsmaßnahmen sollten Sie ergreifen, um Cyberattacken auf Ihre IoT-Geräte zu verhindern?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip aus. Keine, eine, mehr als eine oder alle Optionen können wahr sein

- Homomorphe Verschlüsselung installieren.
- Installieren Sie Firewalls.
- Fragmentierungsredundanzstreuung schaffen.
- **Standardpasswörter des Routers ändern.**
- **Deaktivieren Sie nicht genutzte Funktionen in meinem intelligenten Gerät.**
- **Deaktivieren Sie den Fernzugriff auf das Smart-Gerät.**

Situation: Was sollten Sie tun, um ein Superagent der Cybersicherheit zu werden?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip aus. Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Lernen Sie, wie man programmiert, um IoT-Geräte zu verschlüsseln.
- Einen Kontingentplan nach den 4 W's aufstellen: "Was wird erzeugt?", "Wo werden Daten gespeichert?", "Wann werden Daten verwendet?" und "Mit wem werden Daten geteilt?
- **Richten Sie einen Kontingentplan im Anschluss an die 4 W's ein: "Wen soll ich anrufen?" "Wie gehe ich vor?", "Wann sollen andere alarmiert werden?" und "Welche Aktivitäten sind Vorfälle?**
- Beziehen Sie meine ganze Familie, Gleichaltrige und MitarbeiterInnen in das Bewusstsein für Cybersicherheit ein.
- Entwickeln Sie den Plan für die Reaktion auf Vorfälle erst nach einer Sicherheitsverletzung, denn nur so können Sie die richtigen Maßnahmen für die noch bevorstehenden Vorfälle kennen.