BIG DATA und das Internet der Dinge

Neben „Big Data“ ist das Internet der Dinge – auf Englisch „Internet of Things“ (IoT) bezeichnet – eins der großen Zukunftsthemen in der Informatik. In diesem Dossier wird BEE SECURE erklären, was Big Data mit dem IoT zu tun hat, wie sich beide Phänomene gegenseitig beeinflussen und welche Gefahren und Chancen sich aus diesem Zusammenspiel ergeben.

Was ist das Internet der Dinge?

Der Begriff „Internet der Dinge“ (IoT) mag abstrakt und ein klein wenig merkwürdig klingen, ist aber schnell erklärt: Beim Internet der Dinge geht es um Geräte oder „Dinge“, die mit dem Internet verbunden sind. Aber sind nicht schon ganz viele „Dinge“ wie Computer, Laptops, Smartphones, Spielekonsolen, usw. mit dem Internet verbunden? Bei IoT geht es in erster Linie nicht um Computer und Handys, sondern vor allem um Alltagsgegenstände wie Kühlschränke, Lampen, Schlösser, Spielzeuge, und sogar Zahnbürsten.

Schätzungen des Marktforschungsinstituts Gartner zufolge waren 2017 8,4 Milliarden vernetzte Geräte online, 31 Prozent mehr als noch 2016. Bis 2020 sollen es sogar 20,4 Milliarden Geräte sein, die mit dem Netz verbunden sein werden.

Was für Beispiele für IoT gibt es?

Die bekanntesten Beispiel für IoT sind im Moment sicherlich die sogenannten „digitalen Assistenten“ wie Alexa von Amazon oder Home von Google. Auch Apple plant ein ähnliches Gerät, das auf „Siri“ basieren soll. Die Geräte sind Lautsprecher mit integrierten Mikrofonen, die auf Sprachbefehle hören und mit der Cloud verbunden sind. Mit ihnen ist es nicht nur möglich, den Wetterbericht abzurufen oder Musik zu hören, sondern sie lassen sich auch mit anderen vernetzten Geräten verbinden. So lässt sich via Sprachbefehl zum Beispiel das Licht von „intelligenten“, vernetzten Glühbirnen ein- und ausschalten.

Andere Anwendungen sind zum Beispiel Thermostate, mit denen die Heizung auch unterwegs reguliert werden kann – wer zum Beispiel früher als gewohnt von der Arbeit heimkommt, kann schon während der Heimreise die Wohnung aufwärmen. Vernetzte Steckerleisten sorgen dafür, dass man auch „dumme“ Geräte über das Internet ein- und ausschalten kann. Die vernetzten Glühbirnen wurden schon weiter oben erwähnt – manche können nicht nur per App ein- und ausgeschaltet werden, auch verschiedene Lichtstimmungen sind möglich. Außerdem gibt es sogenannte „smart locks“, also intelligente Schlösser, die sich mit dem Smartphone aufsperren lassen. Wer auf Sicherheit bedacht ist, kann Überwachungssysteme mit Kamera und Alarmfunktion in sein Haus einbauen – oder einen Sensor, der frühzeitig Gefahren wie Feuer oder Wasserohrbrüche erkennt.

Das IoT hat aber nicht nur in den Haushalt Einzug gefunden: Im Bereich Medizin und Fitness gibt es schon längere Zeit Armbänder, die Daten über ihre Träger_innen sammeln und den aktuellen Gesundheitszustand überprüfen. Auch vernetzte Zahnbürsten sind bereits am Markt. Auch im Bereich der Verkehrsplanung kommt das IoT zum Einsatz: Busse, Züge, Autos, Ampeln, Straßen, usw. werden zunehmend mit Sensoren ausgestattet, oft unter dem Schlagwort „Smart Cities“.

Damit soll ein besseres Zusammenspiel der einzelnen Transportmittel und ein flüssigerer Verkehr erreicht werden. Auch Flugzeuge und Schiffe sammeln enorme Daten – so kann ein Flugzeug, das einen kleinen Defekt bemerkt, sich schon vor der Landung für eine Reparatur im Hangar anmelden.

Wer an Kühe und Felder denkt, denkt nicht unbedingt an IoT, aber auch die Landwirtschaft wird zunehmend digitalisiert. So können Landwirt_innen am Computer überprüfen, ob ihre Felder gewässert werden müssen und welche Kühe wie viel Milch geben oder eventuell Anzeichen von Krankheiten zeigen. Mähdrescher, die den Landwirten vor einem aufziehenden Gewitter warnen und deswegen vom Spritsparmodus auf maximale Leistung wechseln, werden schon eingesetzt.

Wie kommt die Kaffeemaschine ins Internet?

Die allererste Webcam wurde 1991 an der Universität von Cambridge eingerichtet. Das, um nachschauen zu können, ob sich noch Kaffee in der Kaffeemaschine im Pausenraum befinden würde. Um ein 128 Pixel kleines, schwarzweißes Quadrat anzeigen zu können, war damals ein enormer Aufwand nötig: Eine Kamera, ein Computer und eine Verbindung ins Netz. Heute gibt es schon Kaffeekocher, die per App über das Internet fernsteuerbar sind. Von solchen Geräten konnten die Forscher_innen in Cambridge Anfang der 1990er Jahre nur träumen!

Diese Entwicklung haben zwei wichtige technische Errungenschaften möglich gemacht, die grundlegend für das IoT sind: Vernetzbarkeit und Adressierbarkeit.

Die Vernetzbarkeit ist leicht erklärt: Statt Kabel ist es heute ohne Probleme möglich, in beinahe jedes Gerät einen WLAN-Chip oder eine SIM-Karte einzubauen. Wo dies nicht möglich ist, gibt es noch Technologien wie Bluetooth oder Nahfeldkommunikation (NFC oder RFID-Chips, wie sie zum Beispiel beim kontaktlosen Bezahlen mit Karte zum Einsatz kommen).

Die Adressierbarkeit ist ein anderes Problem, das eher mathematischer Natur ist. Vielleicht haben sie schon mal den Begriff „IP-Adresse“ gehört. Im Internet (IP steht für „Internet protocole, Internet-Protokoll") braucht jedes Gerät eine Adresse, die ihm eindeutig zuordenbar ist – so wie jedes Telefon eine eigene Telefonnummer hat. Bis vor wenigen Jahren wurde die IPv4 (die Version 4 von IP) benutzt, ein Format das das aus einer 32-bit langen Nummer bestand, etwa „172.16.254.1.“ Allerdings gibt es nur 4,2 Milliarden IPv4-Adressen – nicht genug für alle Geräte auf der Welt. Zum Glück wurde schon 1995 der Nachfolger entwickelt: IPv6. Diese Version benutzt Adressen, die 128 bit lang sind und wie folgt aussehen: „2001:db8:0:1234:0:567:8:1“ (Beide Beispiele sind übrigens die gleiche Adresse). Damit sind ungefähr 2^{128} verschiedene Adressen möglich – 340 Milliarden Milliarden Milliarden Milliarden, eine Zahl mit 39 Stellen. Das sollten auf sehr lange Sicht genügend Adressen sein.

Was hat das mit Big Data zu tun?

Wahrscheinlich denken Sie es sich zu diesem Zeitpunkt schon: Wenn überall Geräte stehen, die mit dem Netz verbunden sind, fällt eine Unmenge an Daten an. Laut der US-Firma Cisco sollen 2018 durch das IoT 400 Zettabyte Daten anfallen. 2013 waren es lediglich 3,12 Zettabyte. Würde man diese Datenmenge auf DVDs brennen wollen, bräuchte man 10 Billionen der Scheiben dafür.

Um diese enormen Datenberge nutzen zu können, braucht man Rechenzentren, in denen die Daten gespeichert und analysiert werden können – und natürlich die richtigen Big Data-Algorithmen. Das „Big“ in Big Data bezieht sich allerdings nicht nur auf die schiere Menge der Daten, sondern auch auf die Geschwindigkeit, mit der sie generiert werden und auf die unterschiedlichen Arten von Daten: Vom Musikgeschmack der „Alexa“-Nutzer_innen über die Herzfrequenz der Träger_innen von Sportarmbändern bis hin zu dem Gesundheitszustand von vernetzten Kühen.

Diese Daten werden gesammelt, um später in Datenbanken integriert zu werden. Dafür müssen sie teilweise umgewandelt werden und von Messfehlern bereinigt werden. Auch diese Prozesse können mittlerweile von Algorithmen übernommen werden. Später werden die Daten

aufbereitet, so dass sie auch Menschen gut verstehen können, zum Beispiel in Grafiken oder Karten. Eine „smart city“ kann zum Beispiel eine Übersicht darüber erstellen, auf welchen Straßen gerade Stau ist, wo eine Ampel ausgefallen ist oder in welchem Stadtteil die Luftqualität besonders gut oder schlecht ist.

Für manche Anwendungsfälle müssen die Daten sehr schnell aufbereitet werden: Zum Beispiel bei Einbruchsicherungen oder Gesundheits-Armbändern, die z.B. den Herzschlag einer Person überwachen. Teilweise können die vernetzten Geräte daher einen Teil der Analyse schon selbst vornehmen. Ansonsten gilt immer: Alle Daten, die gesammelt werden, werden im Zweifelsfall irgendwo gespeichert und warten auf ihre Auswertung.

Die möglichen Anwendungen für IoT-Daten, die mittels Big Data-Methoden ausgewertet werden, bergen ein enormes Potential: Eine effizientere Landwirtschaft, die weniger Wasser, Dünger und Pestizide benötigt, eine frühzeitige Erkennung von Krankheiten, ein besseres Transportsystem, automatisierte Wohnungen, die sich auf Bedürfnisse ihrer Bewohner_innen einstellen, usw. Die Möglichkeiten sind scheinbar endlos, aber wie bei jeder Technologie gibt es auch beim Internet der Dinge eine Menge Gefahren und Risiken.

Spioniert mein Toaster mich aus?

Wenn Geräte Daten über ihre Nutzer_innen sammeln, muss das nicht immer zu deren Vorteil sein. Neben den Fragen des Datenschutzes ist immer die Gefahr gegeben, dass bei einem Hack oder einem Leak die gesammelten Daten im Netz landen. Die Mikrofone von Amazons Alexa lassen sich zwar ausschalten – es ist jedoch viel praktischer, wenn die digitale Assistentin ständig mithört und sich auf Zuruf aktivieren lässt. Das bedeutet jedoch, dass eventuell auch private Gespräche mitgeschnitten werden. Die Aufnahmen werden nicht von dem Gerät selbst, sondern in Amazons Cloud analysiert. Die Firma behält sich das Recht vor, Stimmaufnahmen zur Verbesserung seiner Dienste zu speichern – die Fälle, in denen die Polizei auf solche Aufnahmen zurückgreift, um beispielsweise einen Mordfall zu lösen, häufen sich. Aber was, wenn ein privates Beziehungsgespräch in der Cloud landet und geleaked wird?

Welche Gefahren die Daten von Fitness- und Gesundheitsarmbändern bergen, wenn sie in die falschen Hände geraten, liegt auf der Hand: Wohl kaum jemand von uns möchte, dass Fremde den eigenen Gesundheitszustand erfahren können. Grundsätzlich sammeln die allermeisten IoT-Geräte Daten, die so einiges über ihre Nutzer_innen aussagen. Auf den ersten Blick ist vielleicht nicht ersichtlich, was zum Beispiel die Daten einer intelligenten Glühbirne über eine Person aussagen – bei näherer Betrachtung zeigt sich jedoch, dass sich damit sehr gut aufzeichnen lässt, zu welchen Zeiten der Nutzer zu Hause ist oder schläft. Würden Einbrecher_innen diese Daten erbeuten, könnten sie sich wochenlange Observation sparen und auf einen Blick herausfinden, wann sich ein Einbruch lohnt.

Neben dem Datenklau gibt es andere Probleme: Weil Millionen IoT-Webcams nicht ausreichend gesichert waren, wurden sie gehacked und als Botnetz für Ddos-Angriffe missbraucht. Damit war es Hackern möglich, fremde Computernetzwerke mittels millionenfachen Anfragen zum Einknicken zu bringen. Auch die Gefahr von Ransomware stellt sich: Wenn der eigene Computer Opfer einer solchen erpresserischen Malware wird, sind im schlimmsten Fall „lediglich“ die eigenen Daten futsch. Wenn jedoch das Thermostat, das Haustürschloss oder die Glühbirnen nicht mehr funktionieren, weil ein Hacker sie übernommen hat und Lösegeld fordert, kann dies mitunter sehr unangenehme bis lebensbedrohliche Folgen haben.

Welche Gegenmaßnahmen gibt es?

Obwohl es schon viele IoT-Produkte gibt, ist die Entwicklung erst am Anfang. Nutzer_innen haben vor allem das Problem, dass es wenig Standards gibt und jeder Hersteller auf sein eigenes System setzt. Die „Talente“ von Amazons Alexa könnten eine erste Konsolidierung in dem Bereich darstellen: Ähnlich wie Apps können IoT-Geräte oder andere Dienste Alexa ein „Talent“ verschaffen, mit dem sich die Steuerung über das Amazon-Gerät integrieren lässt.

Gerade bei billigeren Geräten ist die Gefahr groß, dass nicht unbedingt auf Sicherheit geachtet wurde und veraltete, unsichere Technik zum Einsatz kam. Ob die eigene IoT-Webcam zum Beispiel von einem Botnetz übernommen wurde, ist für technisch nicht versierte Nutzer_innen kaum herauszufinden. Um solchen Gefahren zu entgehen, hilft nur eine ausführliche Recherche vor dem Kauf – und regelmäßiges Updaten der Software.

Datensparsamkeit sollte auch beim Gebrauch von IoT-Geräten oberstes Gebot sein. Das heißt: Die Geräte öfters mal abschalten, wenn dies möglich ist. Gerade digitale Assistenten, die immer „mithören", können zu einer Gefahr für die eigene Privatsphäre werden. Allerdings sollte die Bürde nicht unbedingt bei den Nutzer_innen liegen, sondern beim Hersteller der Geräte. Auf einer Konferenz in Mauritius wurden zwei Dokumente verabschiedet: Die Mauritius Resolution on Big Data und die Mauritius Declaration on the Internet of Things. Beide Resolutionen erkennen an, dass IoT in Verbindung mit Big Data unser Leben leichter machen kann, aber dass die Hersteller dieser Geräte wegen den großen Datenmengen, die sie produzieren und analysieren, eine große Verantwortung tragen.

Zu IoT wurden folgende Punkte festgehalten:

- Selbstbestimmung ist ein wichtiges Recht für alle Menschen
- Daten, die von IoT-Geräten gesammelt werden, sollten als persönliche Daten angesehen und behandelt werden
- Hersteller von IoT-Geräten sollten klar machen, welche Daten sie zu welchen Zwecken sammeln und wie lange sie diese Daten speichern
- Datenschutz sollte schon in den Designprozess dieser Geräte einfließen
- Daten sollten, sofern es möglich ist, auf den Geräten selbst analysiert werden – ansonsten muss eine verschlüsselte Verbindung zur Übertragung genutzt werden
- Datenschutzbehörden sollten die Einhaltung der entsprechenden Gesetze streng überwachen
- Alle Akteure im IoT-Bereich sollten konstruktiv darüber debattieren, welche Implikationen IoT hat und welche Schlüsse daraus gezogen werden sollen

Das Internet der Dinge bietet, gerade im Zusammenhang mit BIG DATA, viele großartige Möglichkeiten. Leider gibt es auch mindestens genauso viele Gefahren, die auf uns lauern können. Wichtig ist deswegen, sich vor dem eventuellen Kauf von Geräten gut zu informieren und wachsam zu bleiben.

Quellen:

- Wikipedia: Trojan Room coffee pot
- faz: Konzerne verbünden sich gegen Hacker
- Wikipedia: IPv6 adress
- An Internet of Things
- Wenn die Kuh per Funk den Landwirt holt
- 10 Real World Applications of Internet of Things (IoT) – Explained in Videos
- 15 Examples of Internet of Things Technology in Use Today
- Internet of Things to generate 400 zettabytes of data by 2018
- The role of big data analytics in Internet of Things
- Ten examples of IoT and big data working well together
- Big data and the Internet of Things: Two sides of the same coin?
- Data Protection Officials Adopt Internet of Things Declaration and Big Data Resolution

Bei Fragen bezüglich des Internetbetrugs
oder der Nutzung des Internet im Allgemeinen,
wenden Sie sich bitte an die BEE SECURE Helpline:

BEE SECURE HELPLINE BERATUNG
Tel: 8002 1234

Herausgeber: BEE SECURE · B.P. 707 · L-2017 Luxemburg
Tel.: (+(+352) 247-86427 · Fax.: Fax: (+ 352) 46 41 86
bee-secure@snj.luwww.bee-secure.lu

THE GOVERNMENT OF THE GRAND DUCHY OF LUXEMBOURG
Co-financed by the European Union Connecting Europe Facility