Kompetenzzentrum
Öffentliche IT

FORSCHUNG FÜR DEN DIGITALEN STAAT

IMPULS ZU SAFETY, SECURITY UND PRIVACY IM INTERNET DER DINGE

Die Kernidee des Internets der Dinge ist die Verknüpfung von »Dingen« der physischen Welt mit digitalen Systemen. Obwohl man vom »Internet der Dinge« (»Internet of Things«, »IoT«) spricht, sind nicht alle diese »Dinge« aus einer technischen Sicht Teil des Internets und manche sind nicht einmal direkt vernetzt. Insbesondere aus der Verknüpfung zwischen digitalen Prozessen und physischer Umwelt wie auch aus der komplexen und dynamischen Vernetzung der Systeme untereinander ergeben sich – nicht immer sofort erkennbare – Herausforderungen für Angriffs- und Betriebssicherheit und für die Privatsphäre betroffener Menschen.

Neubewertung von Risiken

Der große Unterschied des IoT zu herkömmlichen IT-Systemen ist die massenhafte Vernetzung leistungsschwacher Geräte. Im Verbund können gerade derartige Geräte großen Schaden anrichten, weil ihre Schutz- und Überwachungsmöglichkeiten beschränkt sind. Der Vergrößerung des IT-Angriffspotenzials durch den Einsatz von IoT und die neuartige, enge Verknüpfung der IT mit der physischen Welt muss durch eine angemessene Risikobetrachtung für die neu geschaffenen Systeme begegnet werden.

IoT-Anwendungen – als System betrachtet

IoT-Anwendungen werden stets durch ein mehr oder minder komplexes System unterschiedlichster Komponenten – z. B. Sensoren, Kommunikationsinfrastruktur, Datenverarbeitung und Aktoren – realisiert. Für Sicherheitsbetrachtungen zu solchen Anwendungen reicht es nicht aus, die einzelnen Komponenten separat zu betrachten. Wechsel- und Folgewirkungen werden erst bei einer Gesamtbetrachtung des Systems erkennbar.

Personen- und Sachschäden im Fokus

Während die Ergebnisse herkömmlicher Internetnutzung typischerweise die Erfassung, der Transport und die Produktion von Daten waren, greift das Internet der Dinge unmittelbar in die Steuerung physischer Objekte ein. Damit erhöhen sich die mögliche Zahl und Schwere von Personen- und Sachschäden als Folge der Vernetzung (mit und ohne Internetnutzung) erheblich.

Safety nicht ohne Security

Die Betriebssicherheit (Safety) vernetzter und informationstechnisch gesteuerter physischer Systeme hängt stark von der Angriffssicherheit (Security) der eingesetzten informations- und kommunikationstechnischen Komponenten ab: Eine Notabschaltung beispielsweise verliert ihren Wert, wenn es einem Angreifer gelingt, sie außer Betrieb zu setzen.

Neue Risiken für die Privatsphäre

Eine große Zahl vielfältiger Sensoren im öffentlichen Raum und im unmittelbaren persönlichen Bereich sowie deren Verknüpfung zum Internet der Dinge ermöglichen einen umfassenden und detaillierten Überblick über unsere Aktivitäten in der realen Welt. Dieser Überblick stellt einen bisher nie dagewesenen Zugriff auf die Privatsphäre jedes Einzelnen dar. Plattformen, auf denen Daten aus dem Internet der Dinge und der herkömmlichen Internetnutzung zusammenfließen, stellen ein besonders hohes Risiko dar.

Die vielfältigen Einsatzszenarien und Datenquellen sind die Herausforderung

Für das IoT wird eine große Anzahl von Einsatzszenarien und Anwendungen diskutiert. Gerade die Einbeziehung unterschiedlichster Datenquellen und Informationen verspricht besonders effiziente Lösungen für vielfältige Probleme. Neben einer ganzheitlichen Systembetrachtung ist es notwendig, die Sicherheit in den einzelnen Komponenten zu verankern und Schnittstellen zwischen Teilsystemen zur Durchsetzung von Sicherheitsregeln zu nutzen.

NEUBEWERTUNG VON RISIKEN

Das Internet der Dinge ist kein eigenes Netz, sondern in vielerlei Hinsicht eng mit dem »klassischen« Internet verwoben. Es verknüpft dabei die Informationstechnik mit der physischen Umwelt. Durch diese Vielzahl von Verbindungen vergrößern sich Abhängigkeiten sowie das Angriffspotenzial, daher müssen Schwachstellen und Bedrohungen übergreifend betrachtet werden.

Für IoT-Geräte typisch sind geringe Leistungsfähigkeit und Speicherkapazität sowie beschränkte Stromversorgung und Kommunikationsmöglichkeiten. Diese Eigenschaften begrenzen u. a. die Einsatzfähigkeit von Verschlüsselungstechniken zur Angriffsabwehr und von (Selbst-)Überwachungsmechanismen zur Angriffserkennung. Ein weithin bekanntes Beispiel für die Folgen sind aus IoT-Geräten gebildete Bot-Netze wie »Mirai«, die für Angriffe auf Internet-Server bzw. -Dienste benutzt werden.

Seit einigen Jahren wird das Angebot an IoT-Geräten für den Privatkundenmarkt stark ausgeweitet, z. B. im Smart-Home-Kontext. Dabei kommen aus Kostengründen oft nur knapp ausgestattete Hardware und selten aktuelle und intensiv auf Fehlerfreiheit geprüfte Software zum Einsatz. Softwareupdates sind bei vielen IoT-Geräten nicht ernsthaft vorgesehen und, wenn überhaupt möglich, oft nur umständlich zu bewerkstelligen.

Da Angriffe auf IoT-Geräte zum Zweck des Aufbaus von Bot-Netzen nicht unmittelbar deren Nutzer:innen und Betreiber:innen, sondern »nur« Dritte schädigen, fallen sie vielen Betreiber:innen nicht auf und diese sind dementsprechend unkritisch bei der Geräteauswahl. Generell gibt es bei IoT-Geräten derzeit noch weit weniger Druck von Nutzer- bzw. Betreiberseite, sichere Geräte anzubieten, als bei »klassischer« Informationstechnik. Dies begünstigt einen **massiven Anstieg der Zahl und des Anteils schlecht gesicherter Internetgeräte, die für Angriffe missbraucht werden können**.

IoT-Geräte arbeiten in der Regel automatisch. Dies **erschwert die lokale Erkennung eines Gerätemissbrauchs** zusätzlich, da dieser sich nicht mehr (z. B. durch Leistungseinbußen oder verzögerte Kommunikation) gegenüber Benutzer:innen bemerkbar macht. Auch funktionale Probleme können leicht verborgen bleiben, wenn Selbsttest-Funktionen oder die automatisierte Bearbeitung von Fehlern fehlen bzw. wenn keine Anzeige für Fehlermeldungen vorhanden ist oder angezeigte Fehler(codes) unverständlich bleiben.

Auch wenn bei Weitem nicht alle IoT-Geräte direkt am Internet teilnehmen, sondern oft Gruppen von IoT-Geräten – lokale IoT-Netze bzw. IoT-Subnetze[1] – erst über die »Übersetzungsfunktion« eines gemeinsam genutzten Gateways mit anderen Internetgeräten kommunizieren können, treten die Geräte doch häufig individuell bei ihren Kommunikationspartnern in Erscheinung. Dies erschwert die Erkennung und Bekämpfung koordinierter Angriffe durch mehrere »gekaperte« IoT-Geräte. Da zudem lokale IoT-Netze meist einheitlich administriert werden und oft eine größere Zahl identischer Geräte umfassen, ist ein gelungener Missbrauchsangriff auf ein solches Netz häufig bei vielen der lokalen Geräte erfolgreich.

Die Vielzahl der Geräte erleichtert zudem die **Verschleierung von Massenangriffen**, weil diese nicht mehr geballt von vergleichsweise wenigen Geräten, sondern mit geringerer individueller Frequenz von einer weitaus größeren Zahl von Geräten durchgeführt werden. Ein verspätet erkannter Angriff kann die Schadenshöhe erheblich vergrößern.

Spezielles Augenmerk verdienen **koordinierte Brute-Force-Angriffe**[2] auf Authentifizierungssysteme, z. B. bei Online-Kundenkonten. Durch die große Zahl potenzieller Angreifer mit unterschiedlichen Absenderadressen können sich Schutzmechanismen, die auf der zeitweiligen Blockierung verdächtiger Adressen basieren, als endgültig wirkungslos erweisen.

---

[1] Z. B. das IoT-Netz eines Smart Home bzw. ein Subnetz geografisch verteilter Messstationen eines einzelnen Betreibers.

[2] Brute-Force-Angriffe (engl. »rohe Gewalt«) sind im IT-Kontext Angriffe, bei denen lediglich durch die Anzahl und Dichte der Angriffe (und nicht durch eine aufwandsminimierende Strategie) versucht wird, das Angriffsziel zu erreichen, beispielsweise das Passwort für ein Onlinekonto zu knacken. Koordiniert sind solche Angriffe, wenn dazu gezielt mehrere angreifende Komponenten benutzt werden, was die Erkennung des Angriffs erschwert.

IOT-ANWENDUNGEN – ALS SYSTEM BETRACHTET

Die Vernetzung hat erheblich zur Steigerung der Leistung und der Automatisierbarkeit rein digitaler Systeme beigetragen. Das IoT steht nun dafür, durch vernetzte und verteilte digitale Systeme auch die ortsunabhängige, direkte Interaktion mit der physischen Welt zu ermöglichen. Ein Zielbild des IoT sind weitgehend autonome Systeme, die sich notwendige Informationen – sowohl aus der digitalen Sphäre als auch über die physische Welt – selbstständig beschaffen und ihrem Einsatzzweck entsprechend direkt mit ihrer Umwelt interagieren. Solche Systeme können unter anderem als Roboter in der Industrie oder auch als viele kleine nützliche Anwendungen der Smart City sichtbar werden. Ein häufiges Charakteristikum derartiger Systeme ist, dass sie ohne unmittelbares, bewusstes menschliches Zutun aktiviert und gesteuert werden können.

Die Abbildung rechts zeigt schematisch ein exemplarisches IoT-System. Die »Dinge« sind über Zugangsnetze angebunden, Beispiele dafür sind WLAN, Mobilfunk oder auch spezielle IoT-Funknetze (Low Power Wide Area Networks, LPWANs). Die Sensoren und Aktoren sind darüber mit Plattformen verbunden, die üblicherweise auf Cloud-Infrastrukturen realisiert sind. Teil dieses Pfades ist oft eine Verbindungskomponente (Gateway). Sie kann zusätzlich Sicherheitsaufgaben übernehmen, beispielsweise indem sie den Zugriff auf leistungsschwache IoT-Endgeräte[1] begrenzt. Bei den Plattformen kann prinzipiell zwischen IoT-Plattform, Datenplattform und Anwendungsplattform unterschieden werden, in der Praxis sind die Grenzen fließend. Die wichtigste Aufgabe der IoT-Plattform ist die Verwaltung der IoT-Geräte und ihre Begleitung über den Lebenszyklus: Neue Geräte müssen, z. B. über das Herstellen von Sicherheitsbeziehungen, eingebunden und bestehende Geräte hinsichtlich ihrer korrekten Funktionsweise überwacht werden. Die durch den Betrieb von IoT-Geräten erzeugten Daten werden über Datenplattformen gesammelt und ggf. vorverarbeitet, während die Anwendungsplattform als Gegenüber für die App oder einen Webbrowser auf dem Endgerät dient.

Eine konkrete Anwendung beruht nicht unbedingt nur auf eigens erfassten Daten, sondern nutzt ggf. auch Daten aus anderen Quellen. Ein Beispiel ist die Verortung von »Dingen« auf einer Landkarte. In eine Anwendung können zudem Nicht-IoT-Dienste eingebunden werden, bspw. eine Bezahlfunktion. Im Idealfall werden die Komponenten des Internets der Dinge anwendungsübergreifend genutzt. So können beispielsweise die Daten eines Regensensors in einer Verkehrs-, aber auch in einer landwirtschaftlichen Anwendung verwendet werden. Dieses Aufbrechen von einzelnen Anwendungsgebieten und der daraus folgende »Datenreichtum« sollen bestehende Anwendungen verbessern und neue Anwendungen ermöglichen. Gleichzeitig muss dafür Sorge getragen werden, dass die Daten nicht missbraucht werden und keine neuen Angriffsmöglichkeiten durch die Nutzung des IoT entstehen.

Isolierte Sicherheitsbetrachtungen für einzelne beteiligte Geräte oder Komponenten sind bei IoT-Anwendungen noch weniger zielführend als bei »klassischer« Internet-Kommunikation. Sichere IoT-Endgeräte helfen nur, wenn – abhängig vom Anwendungsfall – auch z. B. die gesamte Cloud-Infrastruktur, in der die IoT-Daten gespeichert und verarbeitet werden, mindestens das gleiche Sicherheitsniveau bietet. Es gilt also, die Sicherheit Ende-zu-Ende zu gewährleisten und den gesamten Datenfluss zu betrachten.

Zwischen den beschriebenen Komponenten gibt es diverse Schnittstellen. Die Schnittstellen markieren gleichzeitig auch Grenzen von (Teil-)Systemen, die ggf. durch unterschiedliche Organisationen oder Teile von Organisationen betrieben werden. Dadurch werden diese Grenzen auch zu wichtigen Punkten zur Durchsetzung von Regeln (Policies). Beispielsweise nutzt Mobilfunk mit der SIM-Karte ein bewährtes Sicherheitselement und über die (glaubwürdige) Mobilfunknummer kann der Zugang zu einem IoT-Prozess kontrolliert werden. Ebenso wird der Zugriff auf Datensätze einer Datenplattform häufig nur nach einer Authentifizierung ermöglicht.

[1] Ein IoT-Gerät ist leistungsschwach, wenn es zumindest in einem der Bereiche Verarbeitungsfähigkeit (Prozessorleistung), Kommunikationsfähigkeit (Datenrate) oder Speicherfähigkeit deutlich geringer ausgestattet ist als übliche Internetgeräte.

PERSONEN- UND SACHSCHÄDEN IM FOKUS

Bei dem Einsatz weitgehend autonom agierender IoT-Systeme können Personen- oder Sachschäden verursacht werden, ohne dass ein Mensch in der konkreten Situation gehandelt oder über die konkrete Aktion (mit-)entschieden hat. Die Schäden können dabei auf fehlerhaftem oder unvermeidlichem aktivem »Handeln« oder »Unterlassen« des Systems beruhen.

Die **Anforderungen an IoT-Systeme müssen** stets **vollständig sein**. Die Systeme müssen in der Lage sein, auch in Situationen, in denen keine Schadensvermeidung möglich ist, eine zwar schädigende, aber möglichst folgenarme Alternative umzusetzen. Dazu bedarf es einer Vorgabe für die Auswahl, selbst falls diese zufällig erfolgen soll. Angemessenes Verhalten autonomer Systeme setzt voraus, dass deren Software die jeweilige Situation bereits vorausschauend zumindest klassifizierbar macht und für alle Klassen begründbar geeignete Handlungsanweisungen angelegt sind.

Der **Sicherheitsprüfung** von IoT-Systemen kommt eine besondere Bedeutung zu. Trotzdem können die möglichen Konstellationen mit potenziellen Personen- oder Sachschäden zu umfangreich für eine vollständige Sicherheitsprüfung oder sogar nur lückenhaft bekannt sein. Manche Tests sind zudem wegen der bereits mit dem Test verbundenen Risiken für Menschen oder wichtige Güter unvertretbar. Die Reaktion des Systems im realen Fall wird daher teilweise theoretisch abgeleitet werden müssen. Diese Ableitung wird bei adaptiven selbstlernenden Systemen einen weiteren Unsicherheitsfaktor enthalten, da nicht einmal die Kombination aus Logik (Software) und konkretem Datenbestand vorab geprüft und bewertet werden kann.

Trotzdem wird ein adaptives selbstlernendes System – z. B. eine Sicherheitsabschalteinrichtung einer Produktionsanlage, die aus der Beobachtung eigener Abschaltvorgänge lernt – in vielen kritischen Situationen besser als ein deterministisches System mit gleichem Ausgangszustand reagieren können und selbst ein deterministisches System oft bereits menschlichen Bedienern überlegen sein. Unvollständige Testbarkeit sollte daher nicht zum K.-o.-Kriterium für IoT-Systeme gemacht werden, deren Sicherheit bzw. Schadensvermeidung in vielen alltäglichen Situationen belegt werden kann und dabei dem Handeln menschlicher Akteure überlegen ist.

Es sollte geprüft werden, ob IoT-spezifische **Haftung**sregeln notwendig sind, z. B. ob ein Bedarf besteht, die Gefährdungshaftung auf weitere Gerätetypen auszudehnen, wenn diese in IoT-Systemen eingesetzt werden. In vielen IoT-Kontexten sind schwerwiegende Schadensereignisse denkbar, aber nicht überall existieren Regelungen, die Betroffene angemessen absichern, die ohne ihr Zutun geschädigt wurden.

Für Fremdschäden im Zusammenhang mit dem Betrieb gefährlicher Geräte (z. B. beim autonomen Fahren) greift typischerweise mindestens eine Gefährdungshaftung des Betreibers. Dieser ist dann üblicherweise durch eine Versicherungspflicht (oder eine umfassende Versicherungsmöglichkeit) vor existenzbedrohenden finanziellen Risiken geschützt. Ist ein Rückgriff auf den Hersteller bzw. Importeur berechtigt, dürfte dieser für einen Versicherer vermutlich deutlich einfacher sein als eine direkte Schadenersatzforderung eines Geschädigten.

Abb. 1a: IoT-System Ende-zu-Ende

SAFETY NICHT OHNE SECURITY

Betriebssicherheit (Safety) setzt in IoT-Kontexten zwingend ausreichende Angriffssicherheit (Security) voraus. Aufgrund der geringen Speicher- und geringen oder hoch spezialisierten Verarbeitungskapazität (einfacher) IoT-Sensoren und -Aktoren, sind diese vergleichsweise uninteressant für Internet-typische Angriffe wie Ausspähen geistigen Eigentums, Erpressung durch Blockierung des Datenzugangs (»Verschlüsselungstrojaner«) oder »Diebstahl« von Verarbeitungskapazität für komplexe Berechnungen (z. B. Krypto-Mining).

Andererseits erschweren oder verhindern die genannten Einschränkungen ebenso wie die oft beschränkten Kommunikationsmöglichkeiten oder ein geringes Energiebudget den Einsatz vieler Schutzmechanismen.

Derartige Geräte eignen sich daher aufgrund ihrer großen Anzahl und ihres in der Regel schwachen Zugriffsschutzes besonders gut dafür, sie z. B. für **Denial-of-Service-Angriffe**[1] oder für **Angriffe auf »Mehrheitsentscheidungen«** zu nutzen: Schäden sind möglich, wenn ein Notfallventil wegen eines Angriffs auf die Kommunikationsinfrastruktur relevante Steuerbefehle nicht rechtzeitig erhält und deshalb nicht öffnet bzw. schließt. Ebenso können in einem schlecht geschützten System mit wenigen, aber korrekt signalisierenden Sensoren »lügende Sensoren« dazu führen, dass die korrekten Sensoren überstimmt werden und z. B. bei einem Brand kein Alarm ausgelöst wird. Auch ein einzelner manipulierter Sensor oder Aktor kann bereits erhebliche Schäden hervorrufen, wenn z. B. ohne Brand eine Löschanlage ausgelöst wird. Selbst einfache IoT-Systeme für den privaten Gebrauch sollten daher über angemessene Konfigurierungs-, Autorisierungs- und Authentifizierungsfunktionen verfügen, die nicht nur die Sicherheit ihrer berechtigten Nutzer:innen, sondern auch die **Sicherheit Dritter im Blick haben.**

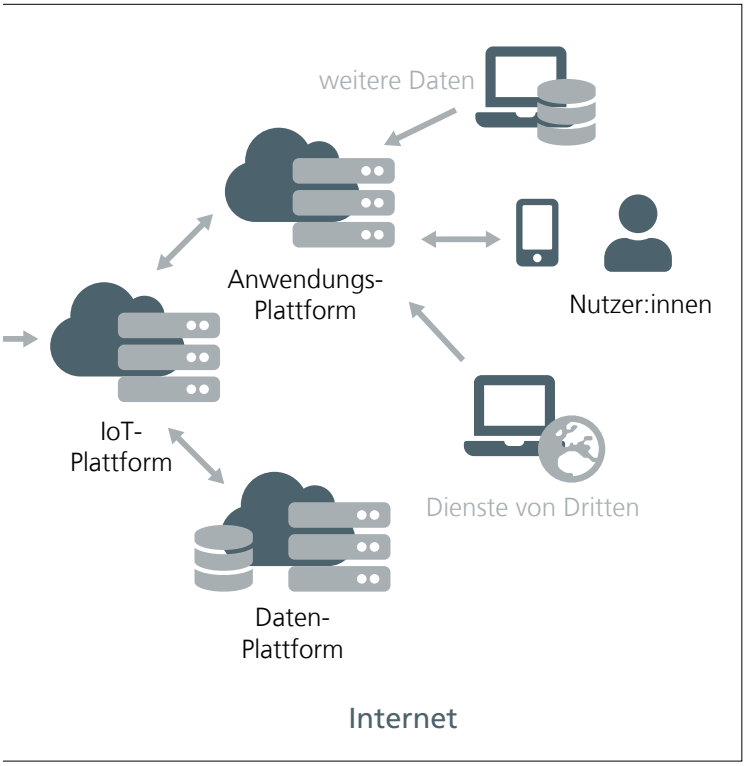

Abb. 1b: IoT-System Ende-zu-Ende

Systeme können manipuliert werden, indem vorhandene Komponenten verändert oder blockiert werden, oder indem – insbesondere bei drahtloser Vernetzung – unberechtigte Komponenten »eingeschleust« werden. Selbst wenn sich eine unberechtigte Komponente beispielsweise als ein bestimmter Sensortyp ausgibt, kann es sich um einen beliebigen (Kleinst-)Computer handeln, der die lokal benutzten Kommunikationsprotokolle beherrscht. Mit den oben genannten Funktionen wird – um die Auswirkungen von Manipulationen zu reduzieren – beispielsweise festgelegt, welche Komponenten überhaupt miteinander kommunizieren dürfen, welche Aktionen sie dabei auslösen dürfen und wie sie ihre Identität und ggf. ihre Unversehrtheit nachweisen müssen. Häufig können solche Funktionen in leistungsstärkeren zentralen Komponenten gebündelt werden.

Dem **Schutz geräte- oder nutzerindividueller Daten** kommt im IoT eine hohe Bedeutung zu, z. B. wenn diese Daten für die Autorisierung oder für die Authentifizierung gegenüber anderen Systemkomponenten benutzt werden. Manipulierte Daten können die Ausführung wichtiger Systemfunktionen verhindern, missbrauchte ausgespähte Daten eine Autorisierung für kritische Funktionen vortäuschen.

[1] Denial-of-Service-Angriff: Über eine Vielzahl von unsinnigen Anfragen wird ein Kommunikationsnetz oder ein daran angeschlossenes Gerät so überlastet, dass das Gerät bzw. sein Dienst (Service) nicht mehr (zuverlässig) für reguläre Anfragen zur Verfügung steht.

NEUE RISIKEN FÜR DIE PRIVATSPHÄRE

Bisher wurden unterschiedliche Bedrohungen der Sicherheit im bzw. durch das Internet der Dinge betrachtet, die dadurch entstehen, dass etwas falsch läuft. Aber auch wenn alle Sicherheitsrisiken sorgfältig betrachtet und entsprechende Maßnahmen ergriffen wurden und die Sensoren korrekte Daten liefern, sind neue Angriffe im Internet der Dinge zu erwarten. Gerade wenn eine Vielzahl von Sensoren detaillierte Informationen bereitstellt, besteht die **Gefahr, dass unbeabsichtigt Informationen abgeleitet und damit offengelegt werden können.** Bspw. wird im Smart Home der plötzliche Abfall der Raumtemperatur mit dem Öffnen von Fenstern zum Lüften assoziiert und der Heizkörper abgestellt. Weitergehend kann auf die Anwesenheit einer Person geschlossen werden (die das Fenster geöffnet hat), woraus wiederum Anwesenheitsmuster erstellt werden können.

Das Problem ist, dass genau die Eigenschaften, die IoT-Systeme so leistungsfähig machen, auch entsprechende fortgeschrittene Angriffe ermöglichen. Das Schließen aus einer Vielzahl unterschiedlicher Daten und die Einbeziehung von Kontextinformationen ermöglichen einerseits clevere Steuerungsalgorithmen, andererseits aber auch fantasievolle Angriffe. Dabei erleichtert das IoT **das gezielte Ausspähen einer Person** (auch durch Strafverfolgungsbehörden) innerhalb einer von IoT-Geräten durchdrungenen Umgebung.

Ähnliches gilt für Plattformen, auf denen die IoT-Daten zusammenlaufen, ausgewertet werden und auf denen die Steuerungsanwendungen laufen. Zur Auswertung werden die Daten zwangsläufig analysiert, daher müssen die Nutzer:innen diesen Plattformen vertrauen können. Problematisch ist in diesem Zusammenhang, dass es im Falle von Datenlecks oder anderen Sicherheitsvorfällen **bei großen Plattformen gleich eine hohe Anzahl von Betroffenen** gibt. Gleichzeitig sind diese Plattformen aber auch ein Ansatzpunkt, um effektiv Sicherheit zu verankern: Von den Betreibern kann erwartet werden, dass sie sichere Systeme aufbauen und betreiben können sowie verlässlich und zeitnah auf nahezu unvermeidliche Sicherheitsvorfälle (Sicherheitslücken, Angriffe) reagieren. Nicht zuletzt können sie dafür sorgen, dass ihre Nutzer:innen zu ihrem eigenen Schutz aktuelle Software einsetzen. Sicherheit und Schutz der Privatsphäre erfordern also sowohl technische als auch organisatorische Maßnahmen. Die Basis bildet dabei verantwortliches Handeln der Anbieter. Dieses muss allerdings ggf. durch Regulierung ergänzt werden, z. B. konkretere Vorgaben für eine nach DSGVO erforderliche Anonymisierung, Pseudonymisierung oder Verschlüsselung.

Eine weitere Form von Angriffen auf die Privatsphäre mithilfe von IoT-Systemen sind beispielsweise gezielte Manipulationen von Smart-Home-Umgebungen, etwa durch Stalker:innen. Wenn Licht oder Geräte scheinbar wie von Geisterhand geschaltet oder die Raumtemperatur manipuliert wird, führt dies in der Regel zu einer großen Verunsicherung der Betroffenen gerade in ihrer privatesten Umgebung, der eigenen Wohnung.

Nicht nur die verteilte Sensorik und Aktorik stellt eine Herausforderung für den Schutz der Privatsphäre dar, auch die vielfach drahtlose Anbindung muss in den Blick genommen werden, selbst wenn verschlüsselt kommuniziert wird. Speziell für das Internet der Dinge eingeführte LPWANs sind darauf optimiert, eine möglichst gute Funkabdeckung zu erzielen (hohe Reichweite bzw. Durchdringung von Wänden) und nur wenig Energie für die gelegentliche Übertragung weniger Daten zu verbrauchen. Sie ermöglichen so die direkte Kommunikation mit energieschwachen (IoT-)Geräten. Beispielsweise für das Fernauslesen von Verbrauchszählern in Haushalten ist das optimal, da keine lokale Infrastruktur (WLAN, Router usw.) mitgenutzt wird. Es gibt dann allerdings auch keinen zentralen Punkt mehr, an dem sich diese Kommunikation einfach sichtbar machen lässt und sie ggf. unterbunden werden kann. Aufgrund des geringen Energieverbrauchs fällt zudem kaum auf, wenn und wie viele Daten unter Einsatz dieser Funktechniken gesendet werden, sodass allgemein nur eine **Kennzeichnung der funkenden Geräte** für die Verbraucher:innen Transparenz schaffen kann.

VIELFALT ALS HERAUSFORDERUNG

Eine Herausforderung für das IoT ist die Anpassung an vielfältige Einsatzszenarien, die eine große Vielfalt von Geräten und Softwarekomponenten notwendig macht. Schon grundsätzliche Fragen wie stationärer oder mobiler Einsatz, die Art der Energieversorgung und notwendige Datenübertragungsraten spannen ein heterogenes Feld von Systemarchitekturen und Kommunikationsprotokollen auf. Die diversen Anforderungen ziehen ganz unterschiedliche technische Lösungen und Kompromisse nach sich. Eine Reduktion der Vielfalt ist also derzeit nicht möglich und auch – trotz technischen Fortschritts – zukünftig nicht zu erwarten.

Diese Vielfalt macht es schwer, einfache Kataloge mit Sicherheitsanforderungen zu erstellen und bspw. Siegel als Ansatz zur Durchsetzung von Mindeststandards einzuführen. Nutzer:innen können auf diese Weise allenfalls einen schnellen Überblick über das Sicherheitsniveau etablierter Geräte(typen) erhalten, die immer neuen Funktionen innovativer Branchen lassen sich auf diese Weise kaum adäquat kategorisieren. Private Nutzer:innen sollten sich an vertrauenswürdigen Herstellern orientieren, die – notfalls aufgrund von Regulierung – Sicherheitsupdates bereitstellen. Für informierte Nutzer:innen sollten (teil-)komponentenspezifische Bewertungen des Sicherheitsniveaus (bspw. für die Komponente »Smart-Home-Gateway« innerhalb eines Heimrouters) zur Verfügung gestellt und mit aktuellen Empfehlungen zum Betrieb (Best Practice) verbunden werden. Das bedeutet auch, dass die Komponenten innerhalb eines Gerätes weitgehend unabhängig sein müssen, um sie getrennt benutzen und ggf. einzeln ersetzen zu können.

Die große Anzahl unterschiedlicher IoT-Geräte nutzt intern eine viel kleinere Anzahl von Chipfamilien, Betriebssystemen, Kommunikationsprotokollen und Softwarebibliotheken. Auch Softwarebibliotheken zur Bearbeitung von Nutzereingaben oder strukturierten Datensätzen sowie Kommunikationsprotokolle sind grundlegende Bausteine, an denen Angreifer ansetzen. Hier können aber ebenso fundamentale Verbesserungen von Sicherheit und Privatsphäre ansetzen, indem gerade diese Bausteine für jedes IoT-Gerät möglichst angriffssicher gestaltet werden und sie zudem die Nutzung von Sicherheitsmechanismen durchsetzen oder möglichst einfach machen. Sind diese Bausteine sicher, kann die Sicherheit von vielen darauf aufbauenden IoT-Geräten verbessert werden.

Es sind diverse Smart-Home-Geräte auf dem Markt, deren Betrieb von Smartphone-Apps und/oder undokumentierten Cloud-basierten Infrastrukturen abhängig ist. Kann man noch naiv davon ausgehen, dass keine Risiken aufgrund unerwünschter Auswertung der Daten und keine Sicherheitslücken drohen, ist jedoch mittelfristig selbst die Nutzbarkeit dieser Smart-Home-Geräte nicht garantiert: Ereignisse wie ein Betriebssystem-Update beim Smartphone (erst recht dessen Wechsel) oder das Abschalten alter Kommunikationsprotokolle durch den Cloud-Betreiber können den Weiterbetrieb von IoT-Geräten verhindern.

In der Praxis führen inkompatible Updates oft auch dazu, dass veraltete und unsichere Software weiterhin genutzt wird. Bei komplexen Systemen im professionellen Umfeld werden veraltete, unsichere IoT-Komponenten auch aus wirtschaftlichen Gründen weitergenutzt, weil deren Ersatz umfangreiche Änderungen oder sogar den Austausch von Teilen der Kommunikationsinfrastruktur bzw. zentraler Datenverarbeitungskomponenten erfordern würde. Demgegenüber können bei einem weitgehend standardkonformen IoT-System mit offengelegten Schnittstellen einzelne Komponenten bei Bedarf gegen sicherere Komponenten ausgetauscht werden.

Die geschilderte Vielfalt an IoT-Kommunikationsprotokollen und -Systemarchitekturen hat auch Vorteile, die gezielt genutzt werden können. Neben technischen oder wirtschaftlichen Vorteilen für bestimmte Anwendungen ist auch die organisatorische Dimension relevant: Durch die gleichzeitige Nutzung verschiedener »Dinge-Netze« findet eine Trennung von Datenströmen statt, bspw. nach verschiedenen Anwendungen oder Typen von IoT-Komponenten. Die dadurch leichtere Erkennung von Anomalien im Netzwerk-Verhalten der Komponenten und die Notwendigkeit von (kontrollierten) Netzübergängen können die Nutzung von IoT-Komponenten sicherer machen. Außerdem können unterschiedliche »Dinge-Netze« als Redundanz genutzt werden: Wenn also ein »Dinge-Netz« aufgrund fehlender Abdeckung oder Ausfall nicht verfügbar ist, so kann die IoT-Anwendung über ein anderes Netz – ob regulär oder in Ausnahmefällen – trotzdem genutzt werden.

DAS INTERNET DER DINGE KOMMT – MACHEN WIR ES SICHER!

Das Internet der Dinge ist anders als man die Automatisierung und Digitalisierung bisher kennt: Sensoren erfassen immer mehr Aspekte unserer Umwelt in bisher nicht dagewesenem Detailgrad, viele uns umgebende Prozesse laufen automatisch ab und aus unscharfen Informationen werden Schlüsse gezogen. Das hat weitreichende Konsequenzen für die Sicherheit der Systeme und auf unsere Privatsphäre.

Umgang mit Daten klar ausgestalten

Beim Internet der Dinge ist es besonders wichtig, dass für alle IoT-Prozesse bekannt ist, welche Arten personenbezogener Daten in welcher Qualität wie und wann verarbeitet werden und welche Auswirkungen das haben kann. Hierzu müssen die Rechte und Pflichten aus der DSGVO und begleitender Regulierung durch klare, verbindliche Regeln für die Dienstanbieter ausgestaltet werden. Spezielles Augenmerk erfordert die Tatsache, dass die Mehrfachverwertung originärer und abgeleiteter Daten – insbesondere auch durch unterschiedliche Beteiligte – einer der Pfeiler der Wertschöpfungserwartungen an das Internet der Dinge ist.

Schnittstellen offenlegen, Hardware und Softwarefunktionen dokumentieren

Alle Schnittstellen von IoT-Geräten sollten grundsätzlich zugänglich und die Hardware zumindest in Grundzügen dokumentiert sein. Die ursprüngliche Software und Betriebsparameter können natürlich technisch und rechtlich geschützt werden, aber in der Regel sollten zumindest Teile der bestehenden Hardware von einer alternativen Software nutzbar sein, insbesondere wenn der Gerätehersteller ein Gerät nicht mehr unterstützt.

IoT-spezifische Forschung zu Softwareentwicklung fördern

Das IoT erfordert Forschung zu sicherer Softwareentwicklung, die die allgemeine Forschungsfrage »Wie können schon durch den Entwicklungsprozess, das Betriebssystem oder andere Systemkomponenten sichere Systeme geschaffen werden?« IoT-Geräte-spezifisch beantwortet. Die geringe Leistungsfähigkeit und Datenkapazität vieler IoT-Geräte erzeugt u. a. große Herausforderungen für kryptografische Schutzmechanismen wie Signieren und Ver-/Entschlüsseln. Hier ist ebenfalls gezielte Forschung erforderlich, die typische IoT-Systemaspekte berücksichtigt.

Strukturierte Netzarchitekturen nutzen und Kommunikation kontrollieren

Sensoren und Aktoren müssen oft nicht direkt mit dem Internet verbunden sein, sondern der Zugriff kann über eine Firewall oder ein besonders gesichertes Gateway erfolgen. Teilsysteme und deren Schnittstellen sind wichtige Ansatzpunkte, um Sicherheit und Nutzungsregeln durchzusetzen sowie unerwünschten Datenverkehr zu unterbinden. Zumindest Gateways zwischen privaten (Firmen-)Netzen und dem Internet sollten daher entsprechende Komponenten beinhalten. Eine derartige Trennung der Netze und die Trennung von Datenströmen auf diesen Netzen (bspw. durch Virtual Private Networks) tragen dazu bei, Angriffe auf schwache und sensible IoT-Komponenten abzuwehren.

In anderen Konstellationen reicht es sogar, dass das Gateway Sensordaten einsammelt und diese über ein Portal im Internet zur Verfügung stellt. Die sensiblen IoT-Geräte selbst kommunizieren dabei nur innerhalb einer abgeschirmten Umgebung. Bevor die Daten eigenen und anderen Anwendungen zur Verfügung gestellt werden, sind so zudem z. B. Plausibilitätschecks (durch das Gateway oder das Portal) möglich. Das Portal als Systemgrenze ermöglicht zusätzliche Kontrolle auch über Dateninhalte. Auf etwaigen Missbrauch kann so schnell und abgestuft reagiert werden.

Autor:innen

Gabriele Goldacker, Jens Tiemann
Kompetenzzentrum Öffentliche IT (ÖFIT)
Tel.: +49 30 3463-7173
Fax: +49 30 3463-99-7173
info@oeffentliche-it.de

Fraunhofer-Institut für
Offene Kommunikationssysteme FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin
www.fokus.fraunhofer.de
www.oeffentliche-it.de
Twitter: @OeffentlicheIT

Gefördert durch:
Bundesministerium des Innern, für Bau und Heimat

Fraunhofer FOKUS

Foto: pixabay, GDJ [0220]