HANDLUNGSFELDER IM BEREICH IOT-SICHERHEIT

Impulspapier | Dezember 2020

Zusammenfassung

Ziel dieses Impulspapiers ist es, Sicherheitsrisiken, die sich durch das Internet der Dinge (Internet of Things, IoT) ergeben, zu diskutieren und Handlungsempfehlungen zum Umgang mit diesen Risiken zu geben. IoT-Geräte sind meist kleine, vergleichsweise leistungsschwache, vernetzte Geräte, welche in allen Lebens- und Produktionsbereichen zu finden sind. Besonders an IoT-Geräten ist, dass sie aufgrund ihrer Allgegenwärtigkeit und Vernetzung nicht nur selbst Angriffen ausgesetzt sind, sondern auch Dritte gefährden können. Ein wesentliches Sicherheitsrisiko ist eine Massenüberwachung der Anwenderinnen und Anwender durch den massenhaften Missbrauch der durch die IoT-Geräte erhobenen Daten. IoT-Geräte können auch ein Einfallstor in das interne Netzwerk darstellen und dieses so gefährden. Fremde Netze können gefährdet werden, wenn IoT-Geräte für verteilte Überlastangriffe (DDoS-Angriff) missbraucht werden. Letztlich können sogar physische Schäden verursacht werden, wenn IoT-Geräte Aktuatoren steuern. Aufgrund dieser vielfältigen Risiken müssen IoT-Geräte besonders gut abgesichert werden. Jedoch unterliegen diese meist sehr kleinen und vergleichsweise günstigen Geräte einem enormen Kostendruck und sehr kurzen Time-to-Market Zyklen, was dazu führt, dass Sicherheit als zunächst unsichtbare Eigenschaft vernachlässigt wird; es kommt zu einem Marktversagen. Da das IoT eine große Chance für wichtige deutsche Industrien wie dem Maschinenbau oder der Haushaltsgeräteindustrie darstellt, ist es auch aus volkswirtschaftlicher Sicht wichtig, dass starke Sicherheitsmechanismen zur Verfügung stehen. Um diese zu erreichen, müssen zunächst Sicherheitsstandards etabliert werden und es bedarf der gezielten Förderung von Sicherheitsforschung für IoT. Diese Förderung muss zum einen gezielt die Besonderheiten von IoT berücksichtigen, auf der anderen Seite jedoch auch für Rechtssicherheit bei Sicherheitsforschung, insbesondere außerhalb von Academia sicherstellen.

Ausgangslage IoT

Der Begriff „IoT“ wird zum Teil unterschiedlich ausgelegt, von daher ist die nachfolgende Definition hilfreich. Wir betrachten die Sicherheitssituation „intelligenter“ Geräte mit den folgenden Eigenschaften:

- Es handelt sich um sogenannte eingebettete Anwendungen oder „Embedded Systems“, d. h. der steuernde Computer („die Intelligenz“) ist in das Gerät integriert. Der Mensch nimmt hierbei primär die Anwendung selber wahr, z. B. einen Fitnesstracker oder ein intelligentes Küchengerät – der Computer tritt in den Hintergrund.
- Die Geräte sind vernetzt, in der Regel kabellos, beispielsweise über WiFi, Bluetooth oder Mobilfunk.
- Die Geräte interagieren zumeist mit ihrer Umwelt, entweder passiv, indem Umgebungsgrößen wie Temperatur oder Blutzuckerspiegel erfasst werden oder aktiv, indem Aktionen wie das Ein- und Ausfahren eines Sonnenschutzes veranlasst werden.
- Die Geräte verfügen über weniger Rechenleistung als heutige PCs oder Laptops.

Der Fokus unserer Betrachtung liegt dabei in erster Linie auf den Geräten selbst und nur nachgelagert auf den Netzwerkaspekten und eventuell zugehörigen Cloud-Services, die bei der Konzipierung und Umsetzung einer vollumfassenden IT-Sicherheitslösung für das IoT ebenfalls berücksichtigt werden müssen. Die Spannbreite der so definierten IoT-Geräte ist sehr groß. Nachfolgend sind, wirklich nur beispielhaft, einige IoT-Anwendungsdomänen genannt: der Smart-Home-Bereich, digitale Sprachassistenten, die Medizintechnik (z. B. ärztliche Diagnosegeräte oder Sensoren zur Glukosemessung) oder auch die intelligente Landwirtschaft. Obwohl der Fokus dieses Impulspapieres auf den eingebetteten Endgeräten liegt, sollte nicht außer Acht gelassen werden, dass diese vernetzt sind. Oft erfolgt die Vernetzung in einem zentralen Serversystem, so dass IoT-Geräte häufig mit der Cloud verschmelzen. Ein prominentes Beispiel ist die Vernetzung der Endgeräte bei der zu Google gehören-

den Firma Nest (u.a. Thermostate, Rauchmelder, Überwachungskameras) für das Smart Home und deren Verbindung über die Google-Cloud.

Cybersicherheit im Kontext von IoT-Geräten weist eine Reihe von Spezifika aus, welche sie von der Sicherheitssituation anderer IT-Strukturen unterscheidet. Zum einen ist das Schadenspotential durch die enge Kopplung an die reale, physische Welt sehr groß. Dieses reicht von bösartigen Manipulationen von Medizinprodukten, welche gesundheitlichen Schäden zur Folge haben könnten, über Produktionsausfällen bei Angriffen auf industrielle IoT-Geräte bis hin zu möglichen massiven Verletzungen der Privatsphäre oder dem Ausspionieren von Geschäftsgeheimnissen. Eine andere Eigenart der IoT-Sicherheit ist, dass Hersteller und Betreiber oft kein Spezialwissen über Cybersicherheit haben. Ein subtileres Problem ist, dass bei allen beteiligten Akteuren – Endnutzern, Betreibern und Herstellern – die Wahrnehmung des IoT-Gerätes als „Cyber-Anwendung" oft nicht ausgeprägt ist und somit die entsprechenden Sicherheitsrisiken auch weniger wahrgenommen werden.

Schadenspotential durch IoT-Angriffe

Verglichen mit traditionellen IT-Systemen birgt das IoT als komplexes Netzwerk miteinander verbundener Geräte verschiedene neuartige Angriffsmöglichkeiten und Gefahren. Dafür gibt es mehrere Ursachen: Zum einen werden viele IoT-Geräte nicht von Grund auf für den vernetzen Einsatz konzipiert und es fehlt „Security by Design", d.h. sie sind oftmals nur unzureichend abgesichert. Sobald eine Schwachstelle gefunden und verbreitet wird, können Angreifer diese von überall auf der Welt ausnutzen und durch die Reichweite und Verbreitung des IoT enorme Schäden verursachen. Schließlich gibt es auf Seiten der Endbenutzer von IoT-Geräten nicht das gleiche Sicherheitsbewusstsein wie dies beispielsweise bei PCs oder Smartphones der Fall ist. Dies führt zusammen mit oftmals komplizierten oder nicht vorhandenen Update-Mechanismen dazu, dass einmal entdeckte Schwachstellen auf den Geräten persistieren. Details zu Sicherheitsupdates und zum Sicherheitslebenszyklus befinden sich im Abschnitt zu den besonderen technischen Rahmenbedingungen der IoT-Sicherheit. Im Folgenden werden einige der durch die Verbreitung des IoT entstandenen neuartigen Bedrohungen erläutert.

Neuartige Angriffsmöglichkeiten

Am naheliegendsten und zugleich besonders gefährlich sind Angriffe auf IoT-Geräte, die durch ihre Aktuatoren selbst direkt in die physische Welt eingreifen, da bei der Kompromittierung eines solchen Geräts ein **physischer Schaden** droht. Dieser wird umso gefährlicher, je kritischer der Einsatzbereich der jeweiligen IoT-Komponente ist. Mögliche Szenarien reichen hier vom Smart Home, in dem durch vernetzte Kameras die Privatsphäre verletzt wird oder durch intelligente Türschlösser ein spurenloser Einbruch ermöglicht wird, über moderne Autos, in deren Bordnetz über die Diagnoseschnittstelle eingedrungen werden kann, um Sicherheitssysteme zu deaktivieren, bis zur Insulinpumpe, die nicht oder falsch dosiert.

In diesem Kontext ist außerdem ein vermehrter Einsatz **IoT-spezifischer Ransomware** denkbar. Im Unterschied zu klassischer Ransomware geht es hier nicht um die Blockade von Daten, wie sie beispielsweise wiederholt bei Angriffen auf Krankenhäuser vorgekommen ist, sondern um eine Sperrung der Gerätefunktion des jeweiligen Gerätes bis zur Zahlung eines Lösegelds. In einem Beispiel aus dem Jahre 2016 wurde dieses Konzept anhand eines internetfähigen Thermostats demonstriert: Das mit der Ransomware infizierte Thermostat heizte den Raum bis zu der (unangenehmen) Temperatur von 37 Grad Celsius auf und verlangte die Zahlung von einem Bitcoin für die Freigabe der Temperatursteuerung. In einem anderen Szenario wurden Heizung und Klimaanlage gleichzeitig betrieben und erzeugten auf diese Weise hohe Energiekosten, bis das Lösegeld bezahlt wurde. Der Einsatz von IoT-Ransomware in Endgeräten ist auch in kritischeren Bereichen, beispielsweise bei Fahrzeugen, in der Industrie oder in der Medizintechnik, vorstellbar.

Gefahren für die Privatsphäre von Individuen bestehen auch durch den potentiellen **massenhaften Missbrauch der von IoT-Geräten gesammelten Daten** oder einer damit verbundenen **Massenüberwachung durch staatliche oder private Akteure**. Die gesammelten Daten bestehen inzwischen nicht nur aus Bildern, Audio- und Videomitschnitten oder Bewegungsdaten, sondern erfassen mehr und mehr Bereiche, wie beispielsweise die persönliche Gesundheit in Form von Vitaldaten oder auch Verhaltensdaten im Straßenverkehr. Diese Daten können einerseits direkt von den Anbietern, welche sich deutschen und europäischen Datenschutzstandards oft entziehen, zweckentfremdet werden, und andererseits über spezielle technische Schnittstellen oder über direkte Angriffe in die Hände von Dritten geraten. Insbesondere die Agglomeration verschiedener Datensätze birgt dabei ein bisher ungeahntes Schadenspotential sowohl für Individuen als auch für die Gesellschaft als Ganzes.

Eine bedrohliche Form **IoT-basierter DDoS-Angriffe** (verteilter Denial-of-Service-Angriffe) trat im Oktober 2016 in Erscheinung. Hierbei wurden eine Vielzahl verschiedener gekaperter IoT-Geräte, wie beispielsweise Drucker, Router, IP-Kameras oder Babyphones, zu einem großen Botnetz

zusammengeschaltet und starteten gleichzeitig DNS-Suchanfragen beim Anbieter „Dyn“. Infiziert wurden die Geräte dabei mithilfe des Schadprogramms Mirai, welches darauf spezialisiert ist, die Sicherheit verschiedener IoT-Geräte mithilfe eines Brute-Force-Ansatzes zu umgehen. Die gleichzeitigen Suchanfragen führten zu einer Überlastung des DNS-Dienstes von Dyn und damit dazu, dass diverse große Internetplattformen und Services (u.a. Amazon, Netflix, Twitter, GitHub) in Nordamerika und Europa für einen Zeitraum von etwa zweieinhalb Stunden nicht wie gewohnt über ihre URLs erreichbar waren. Unsichere IoT-Geräte können also auch – wie in diesem Fall – als Werkzeug für klassische Cyberangriffe missbraucht werden.

Ganz allgemein dienen unsichere IoT-Geräte auch als zusätzliches **Einfallstor in interne Netzwerke**. Wo in der Vergangenheit nur der Heimrouter Konnektivität bot und in vielen Fällen zumindest rudimentär abgesichert werden konnte, sind viele aktuelle IoT-Geräte, z. B. aus dem Smart-Home-Kontext, über diverse Schnittstellen erreichbar und entsprechend verwundbar.

Die hier dargestellten Schadensarten zeigen nur einen kleinen Ausschnitt des denkbaren Schadenspotentials durch Angriffe auf das Internet der Dinge von heute und morgen. Um darauf aufbauend konkrete Handlungsempfehlungen für eine bessere Absicherung des IoT abzuleiten, werden nachfolgend die speziellen wirtschaftlichen und technischen Rahmenbedingungen betrachtet.

Wirtschaftlich-technische Besonderheiten

Bei der Umsetzung digitaler Schutzmechanismen gibt es im IoT-Kontext eine Reihe von Spezifika, die diese erschweren:

1) Ein generelles Hindernis für IoT-Anbieter ist das Fehlen von Standards, nach denen Produkte als „sicher“ eingestuft werden.
2) Ein wichtiger Hemmschuh ist das Marktversagen in Bezug auf sichere IoT-Geräte. Dieses wird durch das inhärente Spannungsfeld zwischen Kostendruck und Time-to-Market einerseits und dem Fakt, dass die Entwicklung und Integration starker Sicherheitsmechanismen sowohl Kosten erzeugen als auch die Entwicklungszyklen verlängern kann, begünstigt. Nicht nur aber besonders bei IoT-Anwendungen kommt die Beobachtung zum Tragen, dass man „Sicherheit nicht sieht”, sprich, es für den Endkunden schwer ist, die Sicherheit entsprechender Geräte einzuschätzen. Hieraus ergibt sich für Anbieter das Problem, den Aufwand für starke Sicherheitsfunktionen entsprechend beim Gerätepreis zu berücksichtigen.
3) Eine Problematik liegt darin begründet, dass Anbieter von IoT-Geräten oft wenig Spezialwissen auf dem Gebiet der Cybersicherheit besitzen. Unter den Anbietern sind viele Unternehmen, deren Wurzeln nicht im IT-Bereich, sondern beispielsweise im Maschinenbau oder der Medizintechnik liegen. Dies kann dazu führen, dass zum einen in den Technikabteilungen der Unternehmen das notwendige Spezialwissen nur ungenügend vorhanden ist, zum anderen fehlt in der Firmenhierarchie möglicherweise die Aufmerksamkeit für das Thema IT-Sicherheit. Ein damit verwandtes Problem besteht darin, dass es Anbieter von IoT-Geräten gibt, die aufgrund ihrer Firmengröße nicht selbst die notwendigen Sicherheitsspezialisten beschäftigen können. Dieses Problem kann beispielsweise bei Mittelständlern, selbst bei den sogenannten Hidden Champions in Deutschland, die nicht aus der IT-Branche stammen, beobachtet werden.

Besondere technische Rahmenbedingungen der IoT-Sicherheit

Generell besitzt jedes im weitesten Sinne sicherheitsrelevante System oder Gerät die **Asymmetrie zwischen Angreifer und Verteidiger**: Während ein Angreifer lediglich eine Schwachstelle finden muss, um das System zu brechen, muss es von dem Verteidiger gegen jeden möglichen Angriff geschützt werden. Dieses Ungleichgewicht wird im IoT-Umfeld zusätzlich verstärkt. Während die Vielzahl der Geräte und deren Verbreitung ein lohnendes Ziel für „Hobby-Hacker” bis hin zu staatlich finanzierten Einrichtungen darstellen kann, werden die Geräte selbst oft unter hohem Kostendruck von vergleichsweise wenigen Entwicklern konstruiert und geschützt. Trotz einer großen Diversität der IoT-Geräte kommen einzelne Modelle bzw. die darin enthaltenden Mikrochips dennoch in sehr großen Stückzahlen auf den Markt. Hinsichtlich der Skalierbarkeit kann sich damit auch ein relativ hoher Aufwand für den Angreifer auszahlen, wenn im Ergebnis direkt eine Vielzahl an Geräten unter die eigene Kontrolle gebracht werden kann. Dieses gilt insbesondere dann, wenn sich die gefundene Schwachstelle über das Internet ausnutzen lässt und keinen physikalischen Zugriff (mehr) erfordert.

Aus technischer Sicht muss man zwischen zwei IoT-Topologien unterscheiden:

- Insbesondere die Einführung des Internetprotokolls IPv6 in Kombination mit 5G ermöglicht auch auf lange Sicht, dass eine Vielzahl von Geräten eine „echte“ Internetadresse besitzen. Dieses ermöglicht eine sicherheitskritische Topologie, bei der IoT-Knoten ohne zentralen Zugangspunkt mit dem Internet verbunden sind und

somit direkt möglichen Angreifern ausgesetzt sind beziehungsweise als Teil eines Botnetzes nach außen kommunizieren können. Die IoT-Endgeräte selbst sind dabei häufig **nicht vollständig autarke Systeme**, sondern auf eine zentrale Auswertung und Reaktion angewiesen. Im Szenario ohne lokalen Zugangspunkt befindet sich diese Auswertung meist beim Hersteller in einer Cloud, und die Geräte führen auch nur die Anweisungen aus, die beim Hersteller generiert werden. Dass Auswertung und Reaktion oft auch auf außereuropäischen Servern geschehen, stellt große Anforderungen an den Datenschutz und die Datensouveränität.

- Die zweite Topologie beschreibt Endgeräte in lokalen Netzen, die über einen lokalen Zugangspunkt mit dem Internet verbunden sind. Dieser Zugangspunkt dient häufig dazu, die einzelnen Knoten zu steuern bzw. deren Daten zu sammeln, vielmals über eine dedizierte Funktechnologie wie Bluetooth, ZigBee oder auch LTE. Aus Sicht eines möglichen Angreifers stellt dieses zentrale Element das wesentliche Ziel dar, es kann aber aufgrund höherer Leistungsfähigkeit auch besser abgesichert und aktualisiert werden.

Unabhängig von der konkreten Topologie weisen IoT-Geräte viele **Sicherheitseigenschaften klassischer eingebetteter Anwendungen auf**: Sie sind im Allgemeinen relativ leicht zugänglich (Smart Home, digitaler Schlüssel, Medizinprodukte etc.) und nicht „unzugänglich" als Server in einem Rechenzentrum. Neben rein netzwerkbasierten Angriffe ermöglicht dies auch eine ganze Reihe physikalischer Angriffe. Zum Beispiel kann durch Beobachten der elektromagnetischen Abstrahlung Rückschluss auf den verwendeten geheimen Schlüssel gezogen werden (sogenannte Seitenkanalangriffe), was je nach Anwendung zu einem vollständigen Sicherheitsverlust des ganzen Systems führen kann.

Entsprechende Gegenmaßnahmen wurden in der wissenschaftlichen Literatur untersucht, werden aber wegen der einhergehenden Kosten und des Zeitaufwandes oftmals nur in Hochsicherheitsanwendungen, wie beispielsweise bei digitalen Zahlungsmitteln, eingesetzt. Für diese Anwendungen vergibt (und fordert) das Bundesamt für Sicherheit in der Informationstechnik (BSI) Zertifizierungen, denen umfangreiche Tests in akkreditierten Prüflaboren vorrausgegangen sein müssen.

An der **Schnittstelle zwischen den IoT-Geräten und ihren Benutzern** liegt eine weitere technische Besonderheit. Klassische Computer werden durch Home-Banking, Passwörter, Antivirussoftware usw. als sicherheitskritisches Gerät wahrgenommen. Insbesondere für IoT-Geräte im Consumer-Bereich ist dieses oft nicht gegeben. Beispielsweise können Lampen mit Internetzugang oft als relativ unkritisch angesehen werden, gleichzeitig können sie jedoch einem Angreifer möglicherweise einen Zugangspunkt in das gesamte Netzwerk geben, oder er kann, wie oben beschrieben, das IoT-Gerät als Bot missbrauchen.

Gleichzeitig sind die Sicherheitsaspekte klassischer Systeme dem Benutzer oft sehr präsent, etwa durch die Anwendung selbst (z. B. Online-Banking), durch reguläre Updates, Sicherheitswarnungen nach Selbsttests oder durch Berichte in der Presse zu Malware und Ransomware. Kleineren IoT-Geräten fehlt es aber oftmals schlichtweg an einer Anzeige, über welche Warnungen zugänglich gemacht werden könnten. Gleichzeitig erfordert das Aufspielen von Sicherheitsupdates in einigen Fällen einen deutlich erhöhten Aufwand als zum Beispiel vollautomatische Software-Updates, die für Laptops und PCs seit langem selbstverständlich sind. Verstärkend wirkt hierbei, dass insbesondere beim Aufbau von Botnetzen das IoT-Gerät selbst gar nicht das Ziel ist und die eingeschleuste Schadsoftware z. B. erst bei ihrem Einsatz als DDoS-Bot im besten Fall bemerkt werden könnte.

Bei der eigentlichen **Entwicklung der Sicherheits-Updates** ergibt sich auch ein weiterer fundamentaler Unterschied: Betriebssysteme und Standardsoftware werden von großen Herstellern mit viel Energie entwickelt und auch gewartet, sodass diese eine hohe initiale Sicherheit aufweisen und erforderliche Updates schnell entwickelt werden können. Weiterhin sind auch Meldeadressen bzw. -prozesse für gefundene Sicherheitsschwachstellen etabliert, sowohl bei den Herstellern selbst, als auch durch unabhängige Dritte (z. B. Behörden oder Vereine). Gleichzeitig haben immer mehr der großen Hersteller sogenannte Bug-Bounty-Programme, die eine Meldung von Sicherheitslücken monetär entlohnen, auch um den Anreiz, diese im Darknet zu verkaufen, zu unterdrücken. Die genannten Sicherheitsmerkmale sind insbesondere für die Vielzahl an kleineren Herstellern auf dem IoT-Markt nicht etabliert. Ein weiterer Aspekt ist, dass Hersteller von IoT-Endgeräten häufig auf Software-Bibliotheken von Drittanbietern zurückgreifen. Damit ist es dem Hersteller meist nicht möglich zu beurteilen, ob das eigene Produkt von einer Sicherheitslücke einer Bibliothek betroffen ist – und dem Endbenutzer erst recht nicht.

Regulatorische Rahmenbedingungen der IoT-Sicherheit

Besonders wichtig für eine erfolgreiche Umsetzung der Handlungsempfehlungen ist eine **Abstimmung der regula-**

torischen Maßnahmen auf internationaler bzw. europäischer Ebene. Hierbei sollten auch Regelungen für spezielle IoT-Anwendungsdomänen (z. B. Hausautomation, Automobilbranche etc.) und deren gesonderte Anforderungen berücksichtigt werden. Auf diese Weise können entsprechende Vorgaben und Standards der beteiligten Akteure – z. B. Hersteller, Betreiber, Endnutzer – etabliert werden.

Das Bewusstsein gegenüber möglichen Sicherheitsgefahren und entsprechenden Lösungen sollte auf allen Ebenen gestärkt werden: Zum einen sollte eine breite Schulung hinsichtlich IT-Sicherheitsthemen der Bevölkerung verstärkt und vereinheitlicht werden, in Form von Kampagnen, als schulische Ausbildung, als fester Bestandteil sowohl von technischen als auch von nicht technischen Berufsausbildungen und Studiengängen, bis hin zu VHS-Kursen für Endanwender. Ein weiterer Punkt ist **die gezielte Förderung von IoT-Sicherheitsforschung**, um Lösungsansätze in offenen Spannungsfeldern zu entwickeln, beispielsweise Sicherheit by Design gegenüber agilen und auf Angriffe reagierenden Sicherheitslösungen. Effiziente Lösungen in diesen Bereichen können insbesondere durch eine verstärkte interdisziplinäre Ausrichtung der IT-Sicherheit erreicht werden, beispielsweise durch die verstärkte Zusammenarbeit von IT-Sicherheitsforschern mit Ökonomen oder Medizinern. Zum anderen sollte unabhängig von einem eventuell fehlenden Sicherheitsbewusstsein der Benutzer Sicherheit und Schutz der Privatsphäre standardmäßig gefordert werden („Security and Privacy by Default"): Hersteller und Anbieter müssen ab Werk die sicherheits- und datenschutzfreundlichste Voreinstellung wählen. Andere Nutzungsmöglichkeiten müssen gezielt durch den Benutzer verändert werden, inklusive entsprechender Warnhinweise.

Ein weiteres entscheidendes Handlungsfeld besteht in der **Verbesserung der rechtlichen Lage von IT-Sicherheitsforschung**. Forscher müssen die Möglichkeit haben rechtssicher offensive Sicherheitsforschung an kommerziellen Geräten durchführen zu können, und müssen dadurch entdeckte Schwachstellen nach einem Responsible-Disclosure-Prozess mit dem Hersteller auch veröffentlichen dürfen. Nur auf diese Weise können auch weiterhin effektiv Schutzmaßnahmen gegen neuartige Angriffe und Sicherheitslücken entwickelt werden. Je nach Kritikalität der Schwachstelle(n) ist auch ein Coordinated Vulnerability Disclosure denkbar, also dass unabhängige Stellen in die Veröffentlichung mit einbezogen werden müssen.

Die Einführung und vor allen Dingen die Durchsetzung einheitlicher **verbraucherfreundlicher Standards beim Datenschutz für IoT-Geräte** stellt ein zentrales Handlungsfeld dar. Dies beinhaltet sowohl strikte Limitierungen für das Sammeln und die Verwendung von Nutzerdaten, als auch ein Recht auf Löschung und Herausgabe der eigenen Daten zum Zwecke eines Anbieterwechsels. Hierbei sollten alle möglichen Aspekte des Datenschutzes betrachtet werden, also insbesondere die Zweckbindung der erhobenen Daten, die Erforderlichkeit der Verarbeitung personenbezogener Daten, der Zugangs- und Zugriffsschutz und eine datenschutzfreundliche Architektur (daher eine Verarbeitung personenbezogener Daten im Endgerät sofern möglich).

Ein Ansatz zur Überprüfung solcher Standards besteht in der Einführung einheitlicher Zertifizierungen für IoT-Geräte, die von einer unabhängigen Instanz durchgeführt werden und neben der Einhaltung der grundlegenden Datenschutzstandards auch einige der oben erwähnten technischen Aspekte berücksichtigen. Der Inhalt einer möglichen Zertifizierung und deren Verbindlichkeit sollte differenziert nach bestimmten Bereichen (Systemarchitektur, Sicherheitseigenschaften etc.) und Anwendungen (Smart Home, Wearables etc. bzw. auch Sensor oder Akteur) erfolgen.

Für den Endkunden können die wesentlichen Zertifizierungsmerkmale durch einheitlich gestaltete IoT-Labels transparent gemacht werden. Diese ermöglichen einerseits dem Verbraucher den Vergleich verschiedener Produkte auf einen Blick, und dienen andererseits als zusätzliches Verkaufsargument für Hersteller, die sich um die Sicherheit und Datenschutzkonformität ihrer Produkte bemühen. Ebenso sollten die Kriterien der Zertifizierung dabei so transparent wie möglich sein, sodass aus einem Siegel eindeutig hervorgeht auf welchen Teil eines Produkts sich die Prüfung bezieht.

Handlungsempfehlungen

Regulatorisch

- Eine zentrale Forderung ist die Einführung und Durchsetzung verbraucherfreundlicher Sicherheitsstandards oder zumindest Richtlinien für IoT-Sicherheit, auf die sich Anbieter und Kunden berufen können. Dieses übergeordnete Ziel sollte in der Cybersicherheitsstrategie verankert werden.
- Standardisierungen sollten mit einem vertretbaren Zeit- und Kostenaufwand für die Hersteller erfüllbar sein.
- In Bereichen, wo Standardisierungen nicht praktikabel sind, wird dem Gesetzgeber empfohlen, eine Produkthaftung durch die Hersteller einzuführen, wenn gewisse Sicherheitseigenschaften nicht erfüllt sind.

- Die Behebung des Marktversagens durch konkrete Vorgaben für die Sicherheit von IoT-Geräten durch den Gesetzgeber, welche auf obenstehenden Sicherheitsstandards bzw. -richtlinien basieren.
- Der Bundesregierung wird empfohlen, eine zentrale Anlaufstelle für IoT-Sicherheitsvorfälle einzurichten. Hier können Punkte wie Schwachstellenmeldungen, gemeinsames Notfallmanagement und Disclosure-Prozesse zum Wohle der Allgemeinheit behandelt werden.

Unterstützung von IoT-Anbietern

- Der Bundesregierung wird empfohlen, Weiterbildungsangebote zu fördern, die sich speziell an IoT-Ingenieure in der Industrie richten. Zielgruppe sollten insb. Fachkräfte sein, die die Anwendungsumgebung gut kennen, aber noch keine umfassende Cybersicherheitsausbildung haben.
- Auf der Verbandsebene soll ein deutsches Ökosystem von beratungsorientierten Anbietern aufgebaut werden, die IoT-Unternehmen bei der Planung und Umsetzung von Sicherheitslösungen unterstützen können.

Forschung

- Es wird empfohlen, dass das BMBF bzw. andere Forschungsförderungsorganisationen spezielle Programme entwickeln, die passgenau technische Lösungen für IoT-Sicherheit adressieren. Mögliche Themen sind Security-and-Privacy-by-Design für das IoT, Agilität von Sicherheitslösungen, Sicherheitslebenszyklus oder Datenschutz versus Vernetzung.
- Neben der Technologieförderung von Herstellern von IoT-Geräten sollen zwecks besserer Skalierbarkeit auch Cybersicherheitsunternehmen gefördert werden, die herstellerübergreifend IoT-Lösungen entwickeln.

Wissenschaftliche Arbeitsgruppe Nationaler Cyber-Sicherheitsrat

Seit Oktober 2018 unterstützt die Wissenschaftliche Arbeitsgruppe den Nationalen Cyber-Sicherheitsrat. Sie berät aus Perspektive der Forschung zu Entwicklungen und Herausforderungen im Hinblick auf eine sichere, vertrauenswürdige und nachhaltige Digitalisierung.

Mitglieder der Wissenschaftlichen Arbeitsgruppe sind: Prof. Dr. Claudia Eckert, Dr. Timo Hauschild, Prof. Dr. Jörn Müller-Quade, Prof. Dr.-Ing. Christof Paar (Hauptautor dieses Impulspapiers), Prof. Dr. Gabi Dreo Rodosek, Prof. Dr. Alexander Roßnagel, Prof. Dr. Michael Waidner