März 2017 · Jan-Peter Kleinhans

Strategische IT-Sicherheitspolitik für das Internet der Dinge

Handlungsoptionen für die Politik

Stiftung Neue Verantwortung

Think Tank für die Gesellschaft im technologischen Wandel

Executive Summary

Das vorliegende Papier beschreibt und bewertet verschiedene Handlungsoptionen, die dem Staat derzeit zur Verfügung stehen. Darüberhinaus wird erläutert, welche Besonderheiten sowie Dynamiken des IoT-Markts dabei zu beachten sind. Das Papier baut hierbei auf dem Papier IT-Sicherheit im Internet der Dinge (2016) auf und ist als Weiterentwicklung zu verstehen.

Beim Thema IT-Sicherheit wird staatlichen Institutionen, kritischer Infrastruktur und der Industrie 4.0 viel Beachtung geschenkt. Darüber wird jedoch vergessen, dass Milliarden „smarter" Haushalts- und Entertainmentgeräte – das Consumer Internet of Things (CIoT) – auf den Markt kommen, die eklatante Sicherheitsmängel aufweisen. Die Anzahl internetfähiger Geräte, bei deren Entwicklung nicht auf Sicherheit geachtet wurde, wird stetig anwachsen. Eklatante Sicherheitslücken in CIoT-Geräten haben zwei Folgen: Erstens führen sie dazu, dass Bürgerinnen und Bürger keinen Schutz vor Kriminellen haben und ihre Geräte ausfallen. So sind mittlerweile vernetzte Spülmaschinen[1], Fernseher[2] und Webcams[3] angreifbar. Zweitens werden die Sicherheitslücken von Kriminellen ausgenutzt, um hunderttausende CIoT-Geräte zu kapern, zusammenzuschließen und industrielle Produktionssysteme oder Webseiten von Unternehmen lahmzulegen.[4] IT-Sicherheit im Internet der Dinge wird damit in den kommenden Jahren nicht nur zu einer Herausforderungen für den Schutz der Verbraucher sondern der vernetzten Wirtschaft zugleich.

Aufgrund fehlender ökonomischer Anreize und falsch verteilten Verantwortlichkeiten kann der Markt für IoT-Geräte dieses Problem nicht alleine lösen. Allerdings muss regulierendes Eingreifen durch den Staat die Besonderheiten des Internets der Dinge berücksichtigen, um effektive Regulierungsansätze zu finden.

Als wichtigster Teil einer nachhaltigen IoT-Strategie wird eine europaweit verpflichtende Mindestanforderung an die IT-Sicherheit von CIoT-Geräten gesehen – ähnlich der bestehenden CE-Kennzeichnung. Ein Anfang könnte hier zum Beispiel mit Internetroutern gemacht werden. Regulierungsbedarf gibt es ebenso bei der Frage nach gesetzlichen Vorgaben hinsichtlich Softwaresupport, vor allem für Sicherheitsupdates. Ebenso sollten Verantwortlichkeiten von Distributoren neu geregelt werden, da die überwiegende Zahl von CIoT-Geräten durch ausländische OEM-Hersteller produziert wird. Eine Ausweitung der Produkthaftung auf Software ist im Kern sinnvoll, jedoch derzeit mit vielen rechtlichen Hürden und offenen Fragen verbunden, wodurch es vermutlich nicht erster Schritt einer IoT-Strategie sein sollte.

Erfolgreiche Regulierungsvorschläge müssen dabei vier Eigenschaften des IoT-Markts berücksichtigen: (1) Wenige Sicherheitslücken in ein paar populären CioT-Geräten reichen aus, um hunderttausende Geräte voll-automatisiert mit Malware zu infizieren. (2) Aufgrund mangelnder Einflussmöglichkeiten durch den Benutzer hält sich Malware verhältnismäßig lange auf CIoT-Geräten. (3) CIoT-Geräte eignen sich sehr gut zur Erstellung von Botnetzen. Bei diesen sind Kompromittierter und Geschädigter nicht dieselbe Entität. (4) Im Gegensatz zu klassischen IT-System ist der Mensch mangels Einflussmöglichkeiten auf die Software nicht das „schwächste Glied in der Kette“.

Einleitung

Hinsichtlich der IT-Sicherheit im Internet der Dinge hat der Markt versagt. Besonders offensichtlich wird dies bei Endkundengeräten wie Heimroutern[5], vernetzten Teddybären[6], smarten Glühbirnen[7] oder Überwachungskameras[8] – dem Consumer Internet of Things (CIoT). Bei CIoT-Geräten wird während der Entwicklung kaum Wert auf IT-Sicherheit gelegt. Einmal auf dem Markt, obliegt es der Willkür des Unternehmens, ob das Gerät jemals ein Software-Update erhält. Bei offensichtlichen Sicherheitsmängeln hängt es vollständig vom Hersteller ab, ob diese jemals behoben werden. IT-Sicherheit hat hier den Status eines unbedeutenden Features, mit dem man sich am Markt kaum abheben kann, dessen Entwicklung aber Zeit und Geld kostet. Der Markt wird das Problem der mangelnden IoT-Sicherheit nicht lösen können, da es an ökonomischen Anreizen für Hersteller fehlt bei der Entwicklung auf Security-by-Design zu achten.[9]

Langfristig wird dies fatale Folgen haben, da in einer vollständig vernetzten Welt nicht mehr nur Daten auf dem Spiel stehen. Stattdessen hat ein erfolgreicher Hack nun potenziell direkte physische Auswirkungen – die smarte Glühbirne verweigert den Dienst, ich werde aus meinem Smart Home ausgesperrt oder ich verliere die Kontrolle über mein Auto. Ebenso haben schlecht entwickelte, unsicher konfigurierte und kaum gewartete „smarte“ Geräte direkte negative Auswirkungen auf unsere Wirtschaft. Hunderttausende solcher Geräte werden von Kriminellen in Botnetzen gebündelt und beauftragt Websites oder Produktionssysteme lahmzulegen, Spam zu versenden oder Werbebannerbetrug zu betreiben. Unsichere smarte Geräte sind daher auch ein reales Probleme für die Industrie 4.0. Durch staatliche Regulierung sollten ökonomische Anreize für CIoT-Hersteller gesetzt und Verantwortlichkeiten gerechter verteilt werden.

Ziel dieses Papiers ist es, verschiedene Regulierungsansätze hinsichtlich ihrer potenziellen Effektivität zu beleuchten. Dabei wird bewertet, inwieweit die verschiedenen Ansätze bestimmte Charakteristika des Internets der Dinge adressieren. Zunächst werden daher vier Besonderheiten des Internets der Dinge dargestellt. Für eine ausführlichere Analyse des Marktversagens hinsichtlich IT-Sicherheit im Internet der Dinge, wird an dieser Stelle auf das erste Papier IT-Sicherheit im Internet der Dinge verwiesen.[10] Im zweiten Teil des vorliegenden Papiers werden dann die verschiedenen Handlungsoptionen untersucht.

1. Besonderheiten des Internets der Dinge

Class Breaks

Ist ein CIoT-Hersteller mit einem Produkt erfolgreich, werden schnell mehrere zehn- oder hunderttausend Stück verkauft. Diese Mengen vervielfachen sich nochmals bei OEM- oder White Label-Geräten. Geräte unterschiedlicher Unternehmen basieren hier auf demselben Produkt eines CIoT-Herstellers. Das bedeutet wiederum, dass die Software auf diesen Geräten ebenso praktisch identisch ist. Durch diese hohe Software-Homogenität wird das Internet der Dinge, gerade im Endkundenbereich, weiterhin interessant und lukrativ für Kriminelle bleiben. Derzeit genügt es, wenn Kriminelle Schwachstellen für ein paar populäre CIoT-Produkte findet, um potenziell mehrere hunderttausend Geräte erfolgreich kompromittieren zu können.[11] Dadurch ist es umso wichtiger, Mechanismen zu finden, durch die auch OEM-Hersteller stärker auf Security-by-Design achten.[12]

Persistenz

Ist ein CIoT-Gerät mit Malware infiziert, bleibt diese leicht über Monate erhalten. CIoT-Geräte haben (wenn überhaupt) nur eingeschränkte Wartungs- und Konfigurationsschnittstellen für den Nutzer, wodurch es äußerst schwer fällt, Malware auf dem Gerät überhaupt zu entdecken. Dies ist ein weiterer Unterschied zu gewöhnlichen PCs, bei denen dem Nutzer eine Vielzahl von Analysewerkzeugen zur Verfügung stehen und er potenziell vollständige Kontrolle über die Software des Gerätes hat. Weiterhin wird das Infizieren von CIoT-Geräten mit Malware durch nicht dokumentierte Logins und Schnittstellen deutlich erleichtert. Einige CIoT-Hersteller versehen ihre Geräte mit festvergebenen Standard-Logins (Kombinationen aus Benutzername und Passwort), die dem Nutzer nicht bekannt sind und durch ihn auch nicht geändert werden können. Zum einen ist es dadurch trivial ein Gerät zu re-infizieren. Zum anderen können Geräte durch das simple Ausprobieren von Standard-Logins nun voll-automatisiert infiziert werden – wie dies beispielsweise bei Mirai-Botnetzen geschieht.[13] Selbst wenn ein CIoT-Hersteller ein Software-Update für ein Produkt veröffentlicht, sind bei vielen CIoT-Geräten die Updatemechanismen extrem unkomfortabel oder erst gar nicht vorgesehen.[14] Auch dadurch bleiben CIoT-Geräte im Schnitt deutlich länger infiziert als klassische IT-Systeme.

Kompromittiert vs geschädigt

Da CIoT-Geräte in der Regel sehr leicht zu kompromittieren sind und sich Malware verhältnismäßig lange auf den Geräten hält, sind sie für Kriminelle die perfekte Grundlage, um großflächige Botnetze aufzubauen. Weitere Faktoren sind (1) die immer bessere Internetanbindung auch von Privathaus-

halten, (2) immer leistungsfähigere Hardware der Geräte selbst und der Umstand, dass (3) gerade Router oder Überwachungskameras konstant mit dem Internet verbunden sind. Ganz gleich, für welche Zwecke das Botnetz später eingesetzt wird (Lahmlegen von Websites und Diensten, Werbebetrug oder Versenden von Spam), erleidet der Nutzer des infizierten Gerätes oft keinen Schaden – Kompromittierter und Geschädigter sind also zwei unterschiedliche Entitäten. Der Nutzer weiß oft gar nicht, ob das eigene Gerät überhaupt Teil eines Botnetzes ist und nachts eventuell Websites angreift oder Spam versendet. Dadurch fehlt unter Umständen beim Nutzer ein intrinsisches Interesse an der Sicherheit des Gerätes. Diese Dynamik unterscheidet Botnetze grundsätzlich von anderen Angriffen, bei denen der Kriminelle gezielt versucht, in ein bestimmtes System, einen bestimmten Dienst oder in ein Benutzerkonto einzudringen und dadurch Geschädigter und Kompromittierter ein und dieselbe Person sind.

Faktor Mensch

Gerade in Unternehmen stellen Mitarbeiter oft eine Herausforderung für die IT-Sicherheit dar. Unbekannte USB-Sticks werden mitgebracht, Benutzerrechte des Betriebssystems werden umgangen oder fremde Programme aus dem Internet heruntergeladen. Das Bild des Menschen als schwächstes Glied in der Kette hat sich über Jahrzehnte verfestigt. Hier zeigt sich ein weiterer Unterschied zwischen Unternehmens-IT und IoT-Geräten aus dem Regal. Wie zuvor erwähnt, hat der Nutzer bei CIoT-Geräten oft kaum Einflussmöglichkeiten auf die Software und Konfiguration. In den meisten Fällen besteht eine vollständige Abhängigkeit vom Hersteller, wie dieser das Gerät konfiguriert hat und mit welcher Software es ausgestattet wurde: Man kann vom Benutzer schlecht verlangen, ein Gerät abzusichern, bei dem es nicht-dokumentierte Fernwartungsschnittstellen und Dienste gibt, die durch den Hersteller lediglich durch festvergebene Passwörter geschützt wurden. Ebenso ist der Benutzer auf regelmäßige und zeitnahe Sicherheitsupdates durch den Hersteller angewiesen. Bleiben diese aus, wird ein ehemals gut abgesichertes CIoT-Gerät schnell unsicher und durch Malware infiziert.
Gerade im Endkundenmarkt spielt der „Faktor Mensch“ bei IoT-Geräten daher nur eine untergeordnete Rolle, da selbst der Expertin die Möglichkeiten fehlen, ausreichend Einfluss auf die Software des Gerätes zu nehmen. Hier besteht weitestgehend Abhängigkeit vom Hersteller des Gerätes.

2. Regulierungsansätze

Staatliches Handeln zur Verbesserung der IT-Sicherheit im Internet der Dinge sollte vor allem darauf abzielen, IT-Sicherheit als Anforderung an CIoT-Produkte zu definieren. Hierbei müssen die zuvor dargestellten Besonderheiten des Internets der Dinge berücksichtigt werden, um effektive

Regulierungsansätze zu finden. IT-Sicherheit im Internet der Dinge muss weiterhin als Verbraucherschutz betrachtet und umgesetzt werden. Derzeit sind Verantwortlichkeiten ungerecht verteilt und es wird abgewartet, dass der Markt von selbst ein Problem behebt, obwohl das Risiko zum Großteil durch die Benutzer getragen wird. Im Sinne des Verbraucherschutzes sollten daher Rechte und Pflichten des Verbrauchers in einer vernetzten Welt neu abgewogen werden. Ebenso ändert sich die Rolle des Herstellers, der nicht mehr nur ein Produkt abliefert, sondern zur Gewährleistung der IT-Sicherheit konstante Softwarepflege zu leisten hat. Im Folgenden wird daher analysiert, inwieweit verschiedene Regulierungsansätze die zuvor erwähnten vier Charakteristika des Internets der Dinge berücksichtigen.

Verpflichtende Mindeststandards

Auf europäischer Ebene werden mittelfristig verpflichtende Mindeststandards für IoT-Geräte umgesetzt werden müssen. Die Europäische Kommission arbeitet hier schon in DG Connect an entsprechenden Vorschriften.15 Europa hätte genügend Marktmacht, um eine solche Marktzutrittsbarriere zu etablieren – in ähnlicher Weise geschah dies beispielsweise schon bei der CE-Kennzeichnung. Eine solche europaweit geltende Anforderung an die IT-Sicherheit von CIoT-Geräten ist als Basis-Absicherung zu verstehen. Ziel wäre die Verhinderung voll-automatisierter Infizierung von Geräten aufgrund grober Fahrlässigkeit bei der Softwareentwicklung des Gerätes. Mit genügend Ressourcen könnten smarte Geräte immer noch infiziert werden, allerdings wäre das Erschaffen gigantischer Botnetze für Kriminelle ökonomisch nicht mehr sinnvoll. Da IT-Sicherheit, im Gegensatz zur physischen Produktsicherheit, ein sich bewegendes Ziel ist, sollte ein solcher Mindeststandard dynamische Elemente enthalten: (1) Hersteller werden verpflichtet, für den Zeitraum der gesetzlichen Gewährleistung regelmäßige und zeitnahe Sicherheitsupdates zur Verfügung zu stellen. (2) Der Hersteller verpflichtet sich, gefundene Sicherheitslücken innerhalb von 90 Tagen zu beheben. (3) Der Hersteller bzw. Inverkehrbringer stellt eine zentrale Kontaktstelle zum Melden von Sicherheitslücken und Softwarefehlern zur Verfügung.

Herausforderung eines solchen verpflichtenden Mindeststandards ist zum einen der Anforderungskatalog selbst: Je stärker man auf eine bestimmte Sparte oder Produktgruppe fokussiert (Router, Smartphones, etc.), desto leichter fällt es, sich auf bestimmte Mindestanforderungen an die IT-Sicherheit zu einigen. Die größere Herausforderung ist jedoch die Überprüfung, ob ein bestimmtes Produkt diese Mindestanforderungen erfüllt. Aus Sicht der IT-Sicherheit wäre eine regelmäßige, unabhängige Zertifizierung wünschenswert. Fraglich ist jedoch, ob dieser Ansatz (1) für die Masse an heutigen und zukünftigen IoT-Geräten praktikabel ist. Und ob (2) eine externe,

unabhängige Produktzertifizierung für günstige IoT-Geräte funktioniert, die eine verhältnismäßig kurze Produktlebenszeit besitzen. Gerade für günstigere CIoT-Geräte könnte man sich ebenso an der CE-Kennzeichnung orientieren, bei der der Produkthersteller eine verbindliche Aussage abgibt, dass er sich an die relevanten Standards gehalten hat. Dies ist deutlich schwächer, als eine externe Produktzertifizierung. Gleichzeitig genügt es, um einen Hersteller bei Missachtung des Standards in Haftung zu nehmen.

Produktlebenszeit vs Software-Support

Übliche Haushaltsgeräte wie Kühlschränke, Waschmaschinen und Fernseher haben Produktlebenszeiten von vielen Jahren. Werden diese Geräte zukünftig vernetzt und ein immer größerer Teil ihrer Funktionalität über Software definiert, muss auch diese Software über die gesamte Produktlebenszeit gepflegt werden. Geschieht dies nicht, wird aus einem ehemals „sicheren“ smarten Gerät ein unsicheres, das leicht infizierbar ist. Die Frage ist nun, inwieweit man vom Hersteller verlangen kann, 10 bis 15 Jahre Softwarepflege für eine Waschmaschine, einen Kühlschrank oder eine Heizungsanlage zu geben?

Selbst wenn im Zuge der gesetzlichen Gewährleistung für 2 Jahre Sicherheitsupdates durch den Hersteller zur Verfügung gestellt werden, werden gängige Haushaltsgeräte für viele weitere Jahre in Betrieb sein – mit dann veralteter und unsicherer Software. Bisher gibt es verschiedene Vorschläge, um dieses Problem zumindest abzumildern: (1) Sobald der Hersteller den Softwaresupport für ein Produkt einstellt, muss er dessen Quellcode der Allgemeinheit zugänglich machen, damit sich andere um die weitere Softwarepflege zumindest potenziell kümmern können. (2) Mit Ende des Softwaresupports wird die Internetkonnektivität des Gerätes abgeschaltet und es wird weiterhin lediglich „offline“ betrieben. (3) Mit Ende des gesetzlichen Software-Supports durch den Hersteller wird der Quellcode einem Dritt-Unternehmen übergeben, das sich auf die Softwarepflege „alter“ IoT-Geräte spezialisiert und für diese fortan Softwaresupport leistet. Ganz gleich wie der Regulierer hier entscheidet, muss ein Abwägung zwischen Verbraucherinteressen, Nachhaltigkeit und wirtschaftlichen Interessen der Unternehmen stattfinden.

Verantwortung von Distributoren

Wie zuvor beschrieben, werden gerade im Endkundenmarkt viele IoT-Geräte durch ausländische OEM-Hersteller produziert. Dadurch entstehen u.a. zwei Herausforderungen hinsichtlich IoT-Sicherheit: (1) Findet eine IT-Sicherheitsexpertin eine Schwachstelle in einem Produkt, kann sie diese nur sehr schwer melden, da sie den tatsächlichen Hersteller des Gerätes nicht kennt.

Weiterhin sind (2) die Distributoren nicht für die Software verantwortlich, da diese durch den OEM-Hersteller entwickelt wurde. Beides führt zu deutlichen Schwierigkeiten bei der Behebung von Sicherheitslücken in OEM-Geräten. Daher sollten Distributoren und Inverkehrbringer einen Single Point of Contact für alle von ihnen vertriebenen CIoT-Geräte zur Verfügung stellen, um direkt Sicherheitslücken an den OEM-Hersteller melden zu können.

Außerdem ist über ein erweitertes Rückgaberecht nachzudenken: Wird im Zeitraum der gesetzlichen Gewährleistung eine Sicherheitslücke bekannt und der Hersteller bessert diese nicht in einer bestimmten Zeit aus, sollte der Kunde das Recht haben, das somit mangelhafte (da unsichere) Produkt, an den Distributor zurückzugeben. Zu beachten ist hier, dass ein erweitertes Rückgaberecht vor allem dann effektiv sein wird, wenn Geschädigter gleich Kompromittierter ist: Wurde beispielsweise der eigene Smart-TV durch Ransomware infiziert und somit unbrauchbar, liegt es nahe, dass dieser durch den Nutzer tatsächlich zurückgegeben werden wird. Ist der eigene Router Teil eines Botnetzes, ist es jedoch fraglich, wie effektiv hier die Möglichkeit einer Rückgabe an den Distributor ist, da der Nutzer (1) vom Botnetz nichts weiß und (2) keinen direkten Schaden davonträgt.

Gütesiegel

Ein Gütesiegel für IT-Sicherheit wird derzeit viel diskutiert[16], jedoch ist dieser Regulierungsmechanismus kritisch zu bewerten: (1) Ein Gütesiegel verankert IT-Sicherheit weiterhin als „Feature“ statt als grundsätzliche Anforderung an ein IoT-Gerät. Wie zuvor dargestellt, sollte ein Mindestmaß an IT-Sicherheit – ähnlich der physischen Produktsicherheit – als verpflichtende Anforderung an ein IoT-Gerät gesehen werden, ohne die der Marktzutritt verwehrt werden kann. (2) Selbst wenn ein Gütesiegel auf einer verpflichtenden Mindestanforderung aufbaut, ist es völlig unklar, ob der Verbraucher auf ein entsprechendes Siegel beim Kauf wert legt. (3) Weiterhin kann es Jahre dauern, bis ein Siegel (im Idealfall) einen Ruf und entsprechende Marktmacht aufgebaut hat. (4) Gerade wenn ein staatliches Siegel für IT-Sicherheit erfolgreich ist, wird es Bestrebungen privater Unternehmen geben, eigene Siegel zu veröffentlichen.[17] Dadurch wird für den Verbraucher völlig undurchsichtig, welches Siegel tatsächlich hält, was es verspricht. Diesen Effekt sieht man seit Jahrzehnten bei Nahrungsmitteln und Textilien.

Capacity Building

Aufklärung und Wachsamkeit des Benutzers haben direkte positive Auswirkungen auf die Sicherheit klassischer IT-Systeme. Gerade in Unternehmen liegt daher zurecht ein Fokus auf Capacity Building. Wie zuvor dargestellt, verhält es sich beim Internet der Dinge jedoch deutlich anders. Der Benutzer

hat hier kaum Einflussmöglichkeiten auf die Software und deren Konfiguration. Capacity Building kann sich daher lediglich darauf beschränken, vor den Gefahren unsicherer CIoT-Geräte zu warnen. Der Versuch, Benutzer zu befähigen, derzeitige, unsichere CIoT-Geräte abzusichern, ist jedoch weder sinnvoll, noch effektiv. Zum jetzigen Zeitpunkt sollte der Fokus daher nicht auf Capacity Building liegen, da hierfür die Abhängigkeit des Benutzers vom CIoT-Hersteller zu groß ist und das grundlegende Design heutiger Geräte dem Benutzer kaum Einflussmöglichkeiten gibt.

Ausweitung der Produkthaftung

Bei der „Softwarehaftung" geht es im Kern darum, den Softwarehersteller stärker in die Verantwortung zu nehmen. Immer mehr Funktionalität eines Gerätes ist über Software definiert und diese kann mangelhaft sein. Es scheint jedoch, als wäre die Ausweitung der Produkthaftung auf Software rechtlich aus verschiedenen Gründen schwierig umzusetzen.[18] (1) Zum einen ist völlig unklar, wie der immaterielle Schaden eines Softwarefehlers monetär zu bewerten ist. (2) Ebenso ist die Beweissicherung und Protokollierung verschiedener Softwarezustände schwierig. (3) Es ist unklar, wie mit Open Source Software umzugehen ist, da es hier keinen einzelnen Softwarehersteller gibt. (4) Letztlich ist auch offen, wie man sich der Haftung entziehen kann – zum Beispiel durch Zertifizierung. Dies würde aber bedeuten, dass sich große Softwarehersteller deutlich leichter der Haftung entziehen können (da sie schon entsprechende Zertifizierungsprozesse umgesetzt haben) als kleine und mittelständische Unternehmen.

Die Hoffnung ist auch, dass sich durch Einführung einer Softwarehaftung die Unternehmen gegen einen Schadensfall versichern werden. Die Versicherungen werden sich wiederum die Entwicklungs- und Produktionsprozesse des Unternehmens anschauen und entsprechend hohe Versicherungspolicen ansetzen, falls beim Entwicklungsprozess nicht auf Security-by-Design geachtet wird. Es ist jedoch sehr fraglich, ob sich Versicherungen im dafür notwendigen Maße eigene IT-Sicherheits- und Softwareentwicklungsexpertise einkaufen werden statt, wie in anderen Bereichen auch, über Checklisten und grobe Einschätzungen zu arbeiten. Letztlich birgt Softwarehaftung die Gefahr stark innovationshemmend zu sein, ohne dass zum jetzigen Zeitpunkt absehbar wäre, dass es IT-Sicherheit in der Praxis nachhaltig stärken würde.

3. Zusammenfassung

Das Internet der Dinge ist jung und gerade der CIoT-Markt befindet sich noch in der Entwicklungsphase. Gleichzeitig haben Softwarefehler schon heute potenziell dramatische Auswirkungen. Wird IoT-Sicherheit weiterhin dem Markt selbst überlassen, werden Verbraucher vermehrt das Vertrauen in die Produkte verlieren und das Internet der Dinge wird zumindest im Endkundenmarkt nicht sein Potenzial realisieren können.

Es ist daher Aufgabe des Staates, die Spielregeln und Verantwortlichkeiten klar zu definieren, ohne zu stark innovationshemmend einzugreifen. Produkte sollten sich über Feature differenzieren, nicht jedoch über IT-Sicherheit. Hier sollten Verbraucher ein gesetzlich vorgeschriebenes Mindestmaß an Sicherheit erwarten dürfen. Zentraler Baustein einer nachhaltigen IoT-Strategie sollten daher verpflichtende europaweite Mindestanforderungen an die Sicherheit von IoT-Produkten sein.

Teil dieser Mindestanforderung sollte ebenso eine klar geregelte Software-Supportzeit sein, da konstante Softwarepflege ein elementarer Baustein der IT-Sicherheit ist. Weiterhin sollte über die Verantwortlichkeiten von Distributoren und Inverkehrbringer nachgedacht werden. Hinsichtlich Gütesiegeln sollte sich der Regulierer die Dynamiken in anderen Branchen anschauen (Nahrungsmittel, Textil) und überlegen, ob durch ein Siegel tatsächlich die IT-Sicherheit des CIoT-Marktes signifikant erhöht werden kann.

Letztlich sollte jedoch vor allem ein Anfang gemacht werden. Schon vor einiger Zeit hatte das BSI ein Testkonzept für Breitbandrouter veröffentlicht.[19] Dies könnte ohne weiteres als Grundlage für eine Regulierung von Internetroutern genutzt werden. Router nehmen eine besondere Schnittstellenfunktion in Haushalten ein und ihnen kommt durch VoIP und der Notwendigkeit Notrufe absetzen zu können, eine gesteigerte Kritikalität zu. Daher liegt es nahe, Mindestanforderungen an die IT-Sicherheit von Breitbandroutern zu stellen und so Erfahrungen zu sammeln.[20] Im nächsten Schritt könnten diese Mindestanforderungen dann auf andere Produktgruppen, wie Webcams, Smartphones und weitere CIoT-Geräte ausgeweitet werden.

Endnoten

1 Jens Regel. 2017. "[CVE-2017-7240] Miele Professional PG 8528 - Web Server Directory Traversal". http://seclists.org/fulldisclosure/2017/Mar/63

2 Echo Duan. 2016. "FLocker Mobile Ransomware Crosses to Smart TV". http://blog.trendmicro.com/trendlabs-security-intelligence/flocker-ransomware-crosses-smart-tv/

3 Mark Stanislav und Tod Beardslay. 2016. "HACKING IoT: A Case Study on Baby Monitor Exposures and Vulnerabilities". https://information.rapid7.com/iot-baby-monitor-research.html

4 Europol. 2016. "International Action against DD4BC Cybercriminal Group". https://www.europol.europa.eu/newsroom/news/international-action-against-dd4bc-cybercriminal-group

5 Simon Kenin. 2017. "CVE-2017-5521: Bypassing Authentication on NETGEAR Routers". https://www.trustwave.com/Resources/SpiderLabs-Blog/CVE-2017-5521--Bypassing-Authentication-on-NETGEAR-Routers/

6 Troy Hunt. 2017. "Data from connected CloudPets teddy bears leaked and ransomed, exposing kids' voice messages". https://www.troyhunt.com/data-from-connected-cloudpets-teddy-bears-leaked-and-ransomed-exposing-kids-voice-messages/

7 Eyal Ronen, et al. 2016. "IoT Goes Nuclear: Creating a ZigBee Chain Reaction". http://iotworm.eyalro.net/

8 Brain Krebs. 2016. "Hacked Cameras, DVRs Powered Today's Massive Internet Outage". https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/

9 Bruce Schneier. 2017. "Security and the Internet of Things". https://www.schneier.com/blog/archives/2017/02/security_and_th.html

10 Jan-Peter Kleinhans. 2016. "IT-Sicherheit im Internet der Dinge". https://www.stiftung-nv.de/de/publikation/it-sicherheit-im-internet-der-dinge

11 Pierre Kim. 2017. "Multiple vulnerabilities found in Wireless IP Camera (P2P) WIFICAM cameras and vulnerabilities in custom http server". https://pierrekim.github.io/blog/2017-03-08-camera-goahead-0day.html

12 Bruce Schneier. 2017. “Class Breaks”. https://www.schneier.com/blog/archives/2017/01/class_breaks.html

13 Ben Herzberg, et al. 2016. “Breaking Down Mirai: An IoT DDoS Botnet Analysis”. https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html

14 The Department of Commerce. 2017. “Fostering the Advancement of the Internet of Things”. S.28. https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf

15 European Commission Staff Working Document. 2016. “Advancing the Internet of Things in Europe”. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016SC0110&from=EN

16 Bundesministerium des Innern. 2016. „Cyber-Sicherheitsstrategie für Deutschland“. http://www.bmi.bund.de/DE/Themen/Sicherheit/IT-Cybersicherheit/Cyber-Sicherheitsstrategie/cyber-sicherheitsstrategie_node.html

17 Siehe https://www.siegelklarheit.de/ueber-uns/

18 Gerald Spindler. 2007. “Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären”. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/ITSicherheitUndRecht/Gutachten_pdf.pdf?__blob=publicationFile&v=2

19 Bundesamt für Sicherheit in der Informationstechnik. 2016. “Testkonzept für Breitband-Router”. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Testkonzept-Breitbandrouter.html

20 Marcus Niemitz, Jörg Schwenk. 2015. „Owning Your Home Network: Router Security Revisited“. https://arxiv.org/abs/1506.04112

Über das Projekt

Das Projekt IT-Sicherheit im Internet der Dinge sucht nach ökonomischen Anreizen für IoT-Hersteller, um bei der Entwicklung stärker auf Security by Design zu achten. Hierfür werden in Workshops verschiedene Regulierungsansätze, um solche positiven oder negativen ökonomischen Anreize umzusetzen, diskutiert und analysiert. Im Fokus des Projektes IT-Sicherheit im Internet der Dinge steht daher die Auflösung des Marktversagens hinsichtlich IT-Sicherheit, da durch das Internet der Dinge erstmals nicht mehr nur Daten auf dem Spiel stehen sondern Sicherheitslücken potenziell direkt Leib und Leben bedrohen.

Über den Autor

Jan-Peter Kleinhans verantwortet den Themenbereich IT-Sicherheit im Internet der Dinge bei der Stiftung Neue Verantwortung. Hier arbeitet er an Ansätzen, dem Marktversagen hinsichtlich IT-Sicherheit im Internet der Dinge entgegen zu wirken, um die voranschreitende Vernetzung unserer Wirtschaft und unseres Privatlebens für alle sicher zu gestalten. Jan-Peter ist Fellow der Transatlantic Digital Debates 2016 und im Projektbeirat des Projektes „Trusted Computing – Aufbau von Zertifizierungsinfrastrukturen zur Sicherung von Marktzutritt und Wettbewerb“ des Bundesministeriums für Wirtschaft und Energie (BMWi). Vor seiner Zeit bei der SNV arbeitete er 2013 bei netzpolitik.org. Jan-Peter studierte Kommunikationswissenschaften in Uppsala, Schweden und Wirtschaftsinformatik in Darmstadt.

Kontakt: jkleinhans@stiftung-nv.de

Impressum

Stiftung Neue Verantwortung e. V.
Beisheim Center
Berliner Freiheit 2
10785 Berlin

T: +49 (0) 30 81 45 03 78 80
F: +49 (0) 30 81 45 03 78 97

www.stiftung-nv.de
info@stiftung-nv.de
Twitter: @SNV_berlin

Design:
Make Studio
www.make-studio.net

Layout:
Franziska Wiese

Kostenloser Download:
www.stiftung-nv.de