November 2016 · Jan-Peter Kleinhans

IT-Sicherheit im Internet der Dinge

Handlungsoptionen für Politik und Gesellschaft

Stiftung Neue Verantwortung

Think Tank für die Gesellschaft im technologischen Wandel

Executive Summary

Spätestens die Angriffe der letzten Monate sollten uns verdeutlicht haben, was auf dem Spiel steht, wenn wir uns weiterhin nicht um IT-Sicherheit im Internet der Dinge kümmern. In Finnland fallen die Heizungen ganzer Häuserblocks aus. Populäre Dienste, wie Twitter, Netflix oder Spotify sind in Teilen der USA über Stunden nicht erreichbar. Auch das organisierte Verbrechen nutzt solche Angriffe, um Unternehmen zu erpressen. Wir vernetzen zunehmend alles, ohne dabei auf die Sicherheit zu achten. Das Internet der Dinge verschärft diese Situation noch erheblich, allein aufgrund der schieren Masse an Geräten.

Wie müssen wir also über IT-Sicherheit nachdenken, wenn wir Milliarden autonomer Geräte über das Internet miteinander verbinden? In unserem Papier analysieren wir zunächst, warum der IoT-Markt (Internet of Things) bei IT-Sicherheit versagt hat und warum das Internet der Dinge für Hacker so interessant ist: Es ist derzeit ökonomisch nicht sinnvoll für IoT-Hersteller bei der Entwicklung auf IT-Sicherheit zu achten, da der Markt vor allem Features und Leistungsfähigkeit honoriert, jedoch nicht Sicherheit. So bestehen Informationsasymmetrien, wodurch der Nutzer vollständig von den Aussagen des Herstellers bzgl. IT-Sicherheit abhängig ist und diese kaum überprüfen kann. Und die Möglichkeit der Externalisierung des Risikos seitens des Herstellers führt zu einem Markt, der überschwemmt ist von unsicheren IoT-Geräten. Diese systemischen Unsicherheiten im Internet der Dinge in Verbindung mit dem hohen Verbreitungsgrad bestimmter IoT-Geräte, immer leistungsfähigerer Hardware und ständiger Konnektivität zum Internet, machen IoT-Geräte besonders lukrativ für Hacker. Das müssen wir ändern.

Im zweiten Teil des Papiers diskutieren wir Handlungsoptionen für die Politik. Der Ruf nach Mindeststandards für IoT-Geräte ist groß – sowohl auf europäischer als auch internationaler Ebene. So spricht auch die Bundesregierung in ihrer neuen Cyber-Sicherheitsstrategie 2016 von einer gewissen “Basis-Zertifizierung” und “Gütesiegeln für IT-Sicherheit”. Beide Ansätze werden jedoch nur gelingen, wenn sie von Beginn an europäisch und international vorangetrieben werden, statt deutsche Insellösungen zu erschaffen. Ein Mindeststandard für IoT-Geräte hätte die Chance, das Marktversagen im Internet der Dinge zu adressieren und könnte, ähnlich der CE-Kennzeichnung, unsicheren Geräten den Marktzugang erschweren. Ein darauf aufbauendes IoT-Siegel könnte Versprechen des IoT-Herstellers gegenüber dem Kunden überprüfbar machen. So würden sich IoT-Hersteller über IT-Sicherheit von der Konkurrenz am Markt differenzieren und IT-Sicherheit würde stärker in die Kaufentscheidung einfließen. Eine erweiterte Produkthaftung kann letztlich an den Mindeststandard und das IoT-Siegel anknüpfen und dadurch leichter umsetzbar werden.

Einführung

Bei IT-Sicherheit im Internet der Dinge haben Staat, Unternehmen und Gesellschaft kollektiv versagt. In Liberia, ein Land mit rund 4 Millionen Einwohnern im Westen Afrikas, ist Anfang November 2016 immer wieder das Internet ausgefallen. Was ist passiert? Unbekannte haben die liberianischen Internetprovider über eine Woche hinweg mit Geräten aus dem Internet der Dinge angegriffen.[1] Hunderttausende kompromittierter IoT-Geräte (Internet of Things) sendeten so viele Daten an die wenigen Internetprovider in Liberia, dass deren Infrastruktur unter der Last zusammenbrach. Dieser Angriff war erfolgreich, weil wir sehr gut darin sind Dinge auf der ganzen Welt zu vernetzen und sehr schlecht darin, diese abzusichern. Und Liberia ist nicht alleine. In den letzten Monaten haben wir gesehen, was auf dem Spiel steht, wenn wir weiterhin die Sicherheit im Internet der Dinge ignorieren. Dyn, ein großer US-amerikanischer Internet-Infrastrukturbetreiber wurde ebenso durch eine solche Distributed Denial of Service Attacke (DDoS) angegriffen, wodurch populäre Internetdienste, wie Spotify, Netflix oder Twitter in Teilen der USA für einige Stunden ausfielen.[2][3]

IT-Sicherheitsforscher gehen davon aus, dass dies erst der Anfang ist und solche Angriffe durch das Internet der Dinge zukünftig deutlich mächtiger werden.[4] Auch große Internetprovider können diese Angriffe kaum mehr alleine abwehren, gleichzeitig kann sich jedoch jeder DDoS-Attacken als Dienstleistung einkaufen: So wurden die Websites der deutschen Regierung aus Protest durch DDoS-Attacken angegriffen, als der ukrainische Ministerpräsident 2015 zu Besuch bei Bundeskanzlerin Merkel war. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) berichtet ebenso von DDoS-Angriffen gegen deutsche Finanz- und Versicherungsdienstleister.[5] Auch der deutsche Mittelstand ist betroffen – das organisierte Verbrechen nutzt DDoS-Attacken zur Erpressung und Wettbewerber nutzen sie, um den Ruf des Konkurrenten zu schädigen.[6] DDoS-Attacken sind fast so alt wie das Internet selbst und eine eher krude Art die Verfügbarkeit eines Dienstes oder einer Website zu beeinträchtigen.

---

1 Michael Mimoso. 2016. “Test-Run DDoS Attacks against Liberia cease”. Threatpost. https://threatpost.com/test-run-ddos-attacks-against-liberia-cease/121793/

2 Lorenzo Franceschi-Bicchierai. 2016. “Blame the Internet of Things for Destroying the Internet Today”. Vice Motherboard. https://motherboard.vice.com/read/blame-the-internet-of-things-for-destroying-the-internet-today

3 Aiko Pras, et al. 2016. “DDoS 3.0 - How terrorists bring down the Internet”. http://doc.utwente.nl/100182/

4 BSI. 2015. “Die Lage der IT-Sicherheit in Deutschland”. Bundesamt für Sicherheit in der Informationstechnik. https://www.bsi.bund.de/DE/Publikationen/Lageberichte/bsi-lageberichte.html

Durch das Internet der Dinge sind diese Attacken jedoch sehr leistungsfähig geworden und stellen eine zunehmende Bedrohung für Unternehmen, Staat und Gesellschaft dar.

Aufgrund der gestiegenen öffentlichen Aufmerksamkeit hat die Politik nun die Chance IT-Sicherheit, gerade im Internet der Dinge, nachhaltig zu stärken. IT-Sicherheitspolitik sollte daher strategisch und im internationalen Kontext betrachtet werden statt, wie bisher, vor allem in nationalen Schranken. Wenn dies nicht geschieht, besteht die Gefahr, dass Unternehmen und Gesellschaft das Vertrauen in das Internet der Dinge und die Vernetzung verlieren. Um Handlungsempfehlungen für eine strategische IT-Sicherheitspolitik näher zu kommen, müssen zunächst zwei Fragen beantwortet werden: (1) Warum ist das Internet der Dinge so unsicher? (2) Warum sind IoT-Geräte so lukrativ für Hacker? Anschließend an diese Analyse stellen wir verschiedene Ideen zur Diskussion. IT-Sicherheit ist komplex und es gibt kein Allheilmittel, eine langfristige IT-Sicherheitspolitik wird stattdessen auf eine Kombination verschiedenster Maßnahmen setzen müssen. Genau über diese möchten wir mit Ihnen diskutieren und sehen dieses Papier als Einladung zu einer solchen Debatte.

Marktversagen im Internet der Dinge

Hinsichtlich IT-Sicherheit hat der Markt beim Internet der Dinge versagt, da IoT-Hersteller derzeit keine ökonomischen Anreize haben, auf IT-Sicherheit bei der Entwicklung zu achten. Warum? Beim Kauf von IoT-Geräten Smartphones, Internet-Router oder Smart-TVs – wird auf Features und Leistungsfähigkeit geachtet, da man diese Aspekte in Testberichten und Benchmarks objektiv und kostengünstig analysieren und vergleichen kann: Welches Smartphone hat die beste Kamera? Welcher Internet-Router die größte WLAN-Reichweite? Welcher Smart-TV unterstützt die meisten Videoformate? Da der Markt diese Aspekte von außen objektiv bewerten kann, honoriert er diese. Bei IT-Sicherheit ist dies deutlich schwieriger.

Erstens ist IT-Sicherheit kein statischer Zustand sondern ein fortwährender Prozess: Es werden ständig neue Sicherheitslücken gefunden und Angreifer entwickeln neue Taktiken, auf die der IoT-Hersteller durch Software-Updates möglichst schnell reagieren sollte. Passiert dies nicht, wird aus einem vermeintlich “sicheren” Produkt sehr schnell ein sehr unsicheres.

Zweitens besteht eine Informationsasymmetrie zwischen Hersteller und Kunde: Da man die Qualität der Software von außen nicht ohne weiteres beurteilen kann, muss der Kunde auf die meist nebulösen Aussagen des Her-

stellers vertrauen – nur dieser weiß, ob die Software des Geräts von neu entdeckten Sicherheitslücken betroffen ist und inwieweit diese durch nötige Software-Updates beseitigt werden.[7]

Drittens kann der IoT-Hersteller, gerade im Consumer-Bereich, das Schadensrisiko vollständig externalisieren: Sollte das Gerät durch einen Softwarefehler kompromittiert werden und dadurch ein Schaden entstehen, haftet der Hersteller in der Regel nicht, da die Software ohne Gewährleistung, "so wie sie ist", zur Verfügung gestellt wird.[8]

Viertens vernetzten nun auch Hersteller ihre Geräte, die zuvor keine Erfahrung mit sicherer Softwareentwicklung hatten – Kühlschränke, Fernseher oder Überwachungskameras. Durch die zuvor angesprochenen Aspekte haben sie ebenso keine Anreize die eigentlich nötigen Investitionskosten für sichere Softwareentwicklung zu tätigen. Dadurch werden bei IoT-Geräten sehr viele Fehler wiederholt, die eigentlich in der IT seit vielen Jahren gelöst sind (fehlende Update-Mechanismen, unverschlüsselte Datenübertragung, etc.).[9]

Fünftens kommt gerade beim Internet der Dinge erschwerend hinzu, dass die Nutzer unsicherer IoT-Geräte ebenso nur einen Bruchteil des Risikos tragen. Die meisten Nutzer wissen gar nicht, dass ihr Router oder die Überwachungskamera gehacked wurden, Teil eines Botnetzes sind und in der letzten Nacht wieder an einer DDoS-Attacke beteiligt waren oder Spam versendet haben. Ähnlich der Umweltverschmutzung sind Botnetze volkswirtschaftlich ein Schaden, für jeden einzelnen IoT-Nutzer jedoch nur von marginaler Bedeutung.[10]

Diese fünf Aspekte verdeutlichen das Marktversagen hinsichtlich IT-Sicherheit im Internet der Dinge und warum es gerade für IoT-Hersteller nicht ökonomisch sinnvoll ist, auf IT-Sicherheit bei der Entwicklung zu achten. Diese systemische Unsicherheit im Internet der Dinge erklärt jedoch noch nicht, warum sich Hacker immer stärker auf IoT-Botnetze fokussieren.

7 Daniel R. Thomas, et al. 2015. "Security Metrics for the Android Ecosystem". University of Cambridge. https://www.cl.cam.ac.uk/~drt24/papers/spsm-scoring.pdf

8 Ross Anderson und Tyler Moore. 2006. „The economics of information security." Science 314.5799. http://tylermoore.ens.utulsa.edu/science-econ.pdf

9 Rapid7. 2016. "Comments to 'The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things'". https://www.ntia.doc.gov/files/ntia/publications/rapid7_comments_to_ntia_iot_rfc_-_jun_2_2016.pdf

10 451 Research. 2016. "When things attack: Mirai and the Dyn DDoS attack reveal a disturbing future". https://451research.com/report-short?entityId=90624

Warum Hacker im Internet der Dinge rekrutieren

Da der Markt falsche Anreize setzt, ist die IT-Sicherheit von IoT-Geräten desaströs. Diese systemische Unsicherheit durch einige der zuvor erwähnten Aspekte gilt jedoch nicht nur für das Internet der Dinge sondern für IT-Sicherheit im Allgemeinen. Besondere Charakteristika des Internets der Dinge führen jedoch dazu, dass es für Hacker besonders leicht und lukrativ ist, IoT-Geräte massenhaft zu hacken und in Botnetzen zu organisieren.

Erstens werden IoT-Geräte immer leistungsfähiger und sind oft gut an das Internet angebunden.[11] Heutige Internetrouter, die bei vielen im Wohnzimmer hinter dem Schrank stehen, besitzen ähnlich viel Rechenkraft wie Smartphones vor wenigen Jahren. Durch zunehmend bessere Hardware können IoT-Geräte ebenso immer mehr Software einsetzen, wodurch sie einem Hacker eine leistungsfähige Plattform für diverse Angriffe bieten.

Zweitens sind IoT-Geräte oft konstant mit dem Internet verbunden – im Gegensatz zu PCs und Laptops. Dadurch ist es potentiell leichter zu jeder Zeit auf einen großen Pool an kompromittierten Geräten eines Botnetzes (Zombies) zurückzugreifen.

Drittens ist es für IoT-Benutzer oft schwierig überhaupt zu erkennen, dass ihr Gerät kompromittiert wurde. Entweder, weil sie sich nicht dafür interessieren (Wann haben Sie das letzte Mal nachgesehen, ob es ein Firmware-Update für Ihren Router gibt?) oder weil entsprechende Logs und Schnittstellen gänzlich fehlen. Ist ein IoT-Gerät also einmal kompromittiert, kann der Hacker davon ausgehen, dass ihm dieses für Wochen oder Monate zur Verfügung steht.

Viertens werden IoT-Geräte in großen Stückzahlen hergestellt, die im Laufe der Produktlebenszeit hinsichtlich der Software nur wenig variieren. Wenn einmal eine Schwachstelle in einem populären IoT-Produkt gefunden wurde, lässt sich diese in der Regel in sämtlichen der hergestellten Geräte dieses Typs ausnutzen. So wurde ein Großteil des Datenverkehrs im Zuge der DDoS-Attacke gegen den Internet-Infrastrukturbetreiber Dyn von über Einhunderttausend Überwachungskameras zweier Hersteller ausgeführt.[12]

11 Jan-Peter Kleinhans. 2015. “IT-Sicherheitspolitik: Aktuelle Themen, Entwicklungen und Handlungsfelder”. Policy Brief Stiftung Neue Verantwortung. http://www.stiftung-nv.de/sites/default/files/policy_brief_it-sicherheit.pdf

12 Zach Wikholm. 2016. “When Vulnerabilities travel downstream”. Flashpoint. https://www.flashpoint-intel.com/when-vulnerabilities-travel-downstream/

Hacker müssen daher derzeit nur wenige Schwachstellen in ein paar weit verbreiteten IoT-Geräten finden, um leistungsfähige, globale Botnetze zu erschaffen.

Fehlende Marktanreize treffen so beim Internet der Dinge auf den perfekten Nährboden. Dadurch haben wir schon heute Millionen leistungsfähiger Geräte am Internet, die unsicher entwickelt wurden, schlecht konfiguriert sind und kaum gewartet werden. Die Veröffentlichung des Quellcodes des Mirai IoT-Virus verdeutlicht dies eindringlich: Mirai besitzt lediglich eine Liste aus 60 Standard-Login-Daten, um sich bei IoT-Geräten anzumelden und Kontrolle über diese zu erlangen.[13] Das hat gereicht um mächtige Botnetze zu erschaffen, die beliebige Angriffe ausführen können. Der Mirai-Quellcode steht nun jedem Hacker zur Verfügung, um ihn weiterzuentwickeln und neue Gerätetypen anzugreifen.

Forscher gehen davon aus, dass die verschiedenen, unabhängigen Mirai-Botnetze eine gemeinsame Angriffskapazität von bis zu 75 Terabit/s besäßen.[14] Das ist das 75-fache des Angriffs gegen den Internet-Infrastrukturbetreiber Dyn, der dazu führte, dass in vielen Teilen der USA Twitter, Netflix oder Spotify nicht verfügbar waren. Laut eigener Aussage des DE-CIX, größter Internetknoten der Welt, wird dort eine Reservekapazität von 20 Terabit/s vorgehalten.[15] Wenn wir die IT-Sicherheit im Internet der Dinge nicht nachhaltig verbessern, wird das Problem daher kontinuierlich wachsen. Jegliche Handlungsoptionen müssen somit zwei Fragen adressieren: Wie gehen wir mit heutigen IoT-Geräten um, die schon kompromittiert sind und auch weiterhin leicht zu hacken sein werden? Und wie verbessern wir die Sicherheit zukünftiger IoT-Geräte, damit Hacker nicht mehr so leicht hochleistungsfähige Botnetze erschaffen können?

Handlungsoptionen für Politik und Gesellschaft

Über die DDoS-Angriffe der letzten Monate wurde in den Medien viel diskutiert und ebenso gab es erste Ideen, wie man diesen begegnen könnte. Häufig fokussieren die Ansätze jedoch auf die Symptome (leistungsfähige Botnetze) und nicht auf die zugrundeliegende Ursache (fehlende Marktanreize bei der Entwicklung auf Sicherheit zu achten). So wird in den USA überlegt, ob das FBI unter Umständen kompromittierte IoT-Geräte hacken oder

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

14 siehe Fußnote 9.

15 Benedikt Fuest. 2016. “Diese Attacke war der Testlauf einer mächtigen Cyberwaffe”. https://www.welt.de/wirtschaft/webwelt/article158986045/Diese-Attacke-war-der-Testlauf-einer-maechtigen-Cyberwaffe.html

sogar ausschalten darf, um weitere Angriffe zu verhindern.[16] In eine ähnliche Richtung gehen Überlegungen einiger Sicherheitsforscher, die einen eigenen, "gutartigen" Virus einsetzen würden, um mit Mirai infizierte Geräte zu reinigen und die betreffenden Sicherheitslücken zu schließen.[17] Der Einsatz eines solchen Virus wäre jedoch in vielen Ländern illegal und würde ebenso beträchtliche Kollateralschäden nach sich ziehen, da die Nutzer unter Umständen keinen Zugriff mehr auf ihre Geräte hätten.

Etwas anders gelagert sind die Überlegungen beim Bundesinnenministerium, das wohl über eine Art "digitalen Rettungsschuss" nachdenkt: Die zur Steuerung des Botnetzes notwendigen Command-and-Control-Server (C2) sollen im Zweifelsfall vom Netz genommen werden können. Dies funktioniert jedoch nur, wenn eine solche Operation koordiniert gegen alle C2 eines Botnetzes stattfindet. Auch hier treten Kollateralschäden auf, da die C2 ebenso legitime Dienste und Websites hosten werden. Es ist fraglich wie effizient ein entsprechender Abwägungsprozess für das Abschalten dutzender C2 eines Botnetzes ablaufen würde. In jedem Fall führen diese Ansätze zu einem Wettrüsten, da Hacker ebenso ihre Viren weiterentwickeln und gegen solche Szenarien wappnen werden.

Letztlich sind solche Überlegungen, wie man mit den derzeit unsicheren IoT-Geräten umgehen soll, wichtig und notwendig. Welche Befugnisse sollen Sicherheitsbehörden im Kampf gegen Botnetze haben? Welche Rolle kommt dem Netzbetreiber zu, der meist den größten Überblick über infizierte Geräte und laufende Angriffe hat? Dürfen IoT-Geräte, wenn sie zu unsicher sind, über das Internet abgeschaltet werden und wenn ja, durch wen? Dies ist nur ein kleiner Ausschnitt der Fragen, auf die wir möglichst schnell Antworten brauchen. Denn wir werden uns damit abfinden müssen, dass es auch zukünftig Millionen unsicherer, kompromittierter Geräte im Internet der Dinge geben wird. Gleichzeitig hilft ein solches rein reaktives Auseinandersetzen mit den Symptomen nicht dabei, die IT-Sicherheit zukünftiger IoT-Geräte zu verbessern. Dies wird nur gelingen, wenn die Politik das beschriebene Marktversagen adressiert.

Die Regierungsparteien haben erkannt, dass dringend **die Ursache** mangelnder IT-Sicherheit (nicht nur) im Internet der Dinge bekämpft werden muss –

16 Joseph Cox. 2016. "Should the FBI hack Botnet Victims to save the Internet?". Vice Motherboard. http://motherboard.vice.com/read/should-the-fbi-hack-botnet-victims-to-save-the-internet

17 Fabian A. Scherschel. "DDoS-Rekord-Botnetz Mirai ließe sich bekämpfen – allerdings illegal". heise security. https://www.heise.de/newsticker/meldung/DDoS-Rekord-Botnetz-Mirai-liesse-sich-bekaempfen-allerdings-illegal-3453658.html

fehlende ökonomische Anreize für Hersteller.[18] In diesem Kontext wird allgemein über **Produkthaftung** für Software gesprochen, um Hersteller stärker in die Verantwortung zu ziehen.[19] Dieser Grundgedanke ist gut und richtig, da es hier deutliche Defizite im deutschen Recht gibt, die auch schon seit Jahren bekannt sind.[20] Gerade bei IoT-Geräten ist es sinnvoll den Hersteller stärker in die Verantwortung zu nehmen, da hier oft eine enge Kopplung zwischen Hard- und Software besteht: Bei PCs und Laptops kann der Nutzer fast vollständig Einfluss auf das Betriebssystem und Programme nehmen, bei IoT-Geräten ist das in der Regel nicht möglich. Der Nutzer ist hier in hohem Maße vom Hersteller abhängig, sowohl was Software-Updates als auch Konfigurationsmöglichkeiten betrifft. Daher sollte auch eine höhere Verantwortung und Rechenschaftspflicht beim Hersteller liegen.

Bei Produkthaftung für Software oder Schadensersatzansprüchen handelt es sich jedoch ebenso um einen reaktiven Ansatz, da der Klageweg über die Gerichte verhältnismäßig langsam ist und nicht skaliert. Ebenso wird es schwierig sein ausschließlich über Ausweitung der Produkthaftung ausländische IT-Hersteller zu mehr Sorgfalt bei der Softwareentwicklung zu bewegen. Eine Ausweitung der Produkthaftung oder der Gewährleistungsansprüche auf Hersteller-Software kann daher lediglich ein Baustein einer strategischen IT-Sicherheitspolitik sein und nicht deren zentrales Element. Eine nachhaltige IT-Sicherheitspolitik sollte zusätzlich auf positive Anreize setzen, da sich beide – Haftung und positive Anreize – ergänzen.

Ein konstruktiver Ansatz, um das Marktversagen hinsichtlich IT-Sicherheit im Internet der Dinge zu adressieren, ist eine Kombination aus Mindeststandard und Gütesiegel. Wie eingangs dargestellt fehlt es Herstellern zurzeit an Möglichkeiten sich über IT-Sicherheit zu differenzieren. Daher fließt es nicht in die Kaufentscheidung des Nutzers mit ein. Weiterhin sind die grundlegenden IT-Sicherheitsprobleme von IoT-Geräten keinesfalls neu, sondern es fehlt oft an den rudimentärsten Grundlagen sicherer Softwareentwicklung. Schon eine konsequente Umsetzung solcher würde es Hackern deutlich erschweren voll-automatisiert gigantische Botnetze zu erschaffen. Auf Mindeststandards könnte man sich weiterhin branchenübergreifend einigen, da alle die gleichen Grundprinzipien sicherer Softwareentwicklung imple-

18 SPD-Bundestagsfraktion. 2016. “Stärkung des digitalen Immunsystems”. Positionspapier. http://www.spdfraktion.de/system/files/documents/16-06-21_digitales-immunsystem_beschluss_spd-btf.pdf

19 BMI. 2015. “Für mehr gemeinsame IT-Sicherheit”. Nationaler IT-Gipfel. http://www.bmi.bund.de/SharedDocs/Kurzmeldungen/DE/2015/11/it-gipfel-minister.html

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

mentieren sollten. Vor allem, da Hacker im Zweifelsfall nicht darauf achten, aus welchem Sektor nun ein bestimmtes IoT-Gerät ist (Gesundheit, Energie, Smart Home, etc.), sondern nach weit verbreiteten Geräten mit schwacher IT-Sicherheit suchen – ganz gleich durch wen diese eingesetzt werden.

Hinsichtlich **Mindeststandards für IoT-Geräte** gibt es derzeit in Europa und den USA verschiedene Initiativen: Das Open Web Application Security Project (OWASP) arbeitet an unverbindlichen IoT-Security Guidelines.[21] Die industrienahe Online Trust Alliance hat ein IoT Trust Framework veröffentlicht.[22] Ebenso hat die weltweite Vereinigung der GSM-Mobilfunkanbieter (GSMA) Sicherheitsempfehlungen für das Internet der Dinge veröffentlicht.[23] Die US Handelskammer hatte ein Konsultationsverfahren zu Sicherheit im Internet der Dinge und der Rolle der Regierung durchgeführt und arbeitet nun an weiteren Workshops zu den zentralen Herausforderungen.[24] Ebenso arbeitet die Europäische Kommission an "Trusted IoT Labels" und überlegt in Workshops, wie entsprechende Mindeststandards aussehen müssten.[25] Nicht zuletzt hat das BSI durch sein veröffentlichtes Testkonzept für Breitband-Router ebenso wichtige Arbeit geleistet, die sich teilweise auf IoT-Geräte im Allgemeinen übertragen ließe.[26]

Wenn das Ziel solcher Bemühungen schlanke, offene und international anschlussfähige Mindeststandards sein sollen, gilt es nun diese verschiedenen Initiativen zu verbinden und Ressourcen zu bündeln. Jeglicher Mindeststandard muss die internationale Dimension des IoT-Marktes berücksichtigen und daher auf wenige Seiten passen, kostengünstig umsetzbar sein und ohne monatelange Zertifizierung auskommen. Es geht um den kleinsten gemeinsamen Nenner, denn nichtmals diesen gibt es zur Zeit.

---

21 Open Web Application Security Project. 2016. "IoT Security Guidance". https://www.owasp.org/index.php/IoT_Security_Guidance

22 Online Trust Alliance. 2015. "OTA Announces Trust Framework to Address Internet of Things Risks". https://otalliance.org/news-events/press-releases/ota-announces-trust-framework-address-internet-things-risks

23 GSMA. 2016. "GSMA IoT Security Guidelines – complete document set". http://www.gsma.com/connectedliving/gsma-iot-security-guidelines-complete-document-set/

24 United States Department of Commerce. 2016. "Comments on the Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things". https://www.ntia.doc.gov/federal-register-notice/2016/comments-potential-roles-government-fostering-advancement-internet-of-things

25 Europäische Kommission. 2016. "AIOTI Workshop on Security and Privacy at ETSI Security Week". https://ec.europa.eu/digital-single-market/en/news/aioti-workshop-security-and-privacy-etsi-security-week

26 BSI. 2016. "Testkonzept für Breitband-Router". https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Testkonzept-Breitbandrouter.html

Für Deutschland und Europa bietet sich hier die Gelegenheit die Spielregeln für das Internet der Dinge mit zu definieren und den Markt gleichzeitig für alle sicherer zu machen.

Ein **IoT-Siegel** würde an einen solchen Mindeststandard anschließen. Erstens könnte man, ähnlich der europäischen CE-Kennzeichnung[27], verlangen dass IoT-Geräte in Europa nur eingesetzt werden dürfen, wenn sie ein solches Siegel besitzen und dadurch den erwähnten Mindeststandard umgesetzt haben . Zweitens böte ein Siegel Herstellern die Möglichkeit, sich über IT-Sicherheit von der Konkurrenz zu differenzieren, da sie nun die Chance hätten dem Kunden zu versichern, dass das Produkt hält, was es verspricht. Drittens fiele eine Durchsetzung der Produkthaftung leichter, da sich der Hersteller durch das Siegel, in Verbindung mit einem Mindeststandard, zu gewissen IT-Sicherheitsprinzipien verpflichtet hat. Daher würden sich beide Ansätze, Produkthaftung und Mindeststandard samt IoT-Siegel, sehr gut ergänzen und gegenseitig stärken.

Herausforderung für einen Mindeststandard und IoT-Siegel wäre sicherlich, dass es sich um "statische" Instrumente handelt, die für ein sehr dynamisches Feld, IT-Sicherheit, angepasst werden müssten. Dies kann aber gelingen, indem das Siegel z.B. von IoT-Herstellern verlangt regelmäßige Updates für sicherheitsrelevante Softwarekomponenten zu liefern. Ebenso muss diskutiert werden, wie ein entsprechendes Siegel aussehen könnte: Ob es ähnlich simpel, wie das CE-Siegel ist und ein Produkt dieses entweder hat oder nicht. Oder ob es abgestufter sein sollte, ähnlich dem in der EU vorgeschriebenen Energieeffizienz-Siegel.[28] [29] Dies sind jedoch nachrangige Überlegungen, die nicht davon ablenken sollten, dass ein IoT-Siegel dabei hilft Mindeststandards umzusetzen.

Unabhängig von Mindeststandards und IoT-Siegel muss ebenso adressiert werden, dass es zurzeit noch verhältnismäßig teuer und aufwendig für Unternehmen ist, von Beginn an auf IT-Sicherheit bei der Entwicklung zu achten. Gerade bei Start-Ups spielt es daher kaum eine Rolle. Um IT-Sicherheit nachhaltig zu stärken, könnte daher sicherheitsrelevante Open Source Software durch **staatlich finanzierte, unabhängige Audits** überprüft werden. Dies geschieht beispielsweise schon durch eine finanzielle Förderung des

27 Europäische Kommission. 2016. "CE marking". http://ec.europa.eu/growth/single-market/ce-marking.de

28 Alex Deschamps-Sonsino. 2015. "What does it do? A proposal for connected product labelling.". http://designswarm.com/blog/2015/09/what-does-it-do-a-proposal-for-connected-product-labelling/

29 Boris Adryan. 2015. "Connected Product Labeling". http://iot.ghost.io/connected-product-labelling/

Europäischen Parlaments.[30] Auch in Deutschland wurde in der Vergangenheit sicherheitsrelevante Open Source Software durch das Bundeswirtschaftsministerium[31] und das BSI[32] gefördert, jedoch war dies immer nur sporadisch und ohne kohärente Strategie. Hier gebe es viel Verbesserungspotenzial. Durch solche Sicherheitsaudits und Förderungen wird weitverbreitete, sicherheitsrelevante Software gestärkt und langfristig für jeden einfacher nutzbar.

Ebenso müssen wir bei IT-Sicherheit, gerade in Deutschland, wegkommen von einem "Ingenieurdenken" – der Überzeugung, dass eine Sache sicher ist, wenn man sie nur gut genug plant und entwickelt. Heutige IT-Systeme sind so komplex und eng miteinander vernetzt, dass es immer zu Fehlern kommen wird, allerdings findet man sie alleine nicht mehr. Diese Erkenntnis ist in den USA z.B. deutlich weiter – dort sind sogenannte **Bug Bounty Programme** mittlerweile etabliert. Unternehmen zahlen unabhängigen Hackern Geld, wenn diese – unter Einhaltung bestimmter Bedingungen – gefundene Softwarefehler an das Unternehmen melden.[33]

Diese Mentalität, dass man alleine nicht mehr alle Fehler findet und damit offen umgehen sollte, hat auch Einzug ins Pentagon gehalten. Dieses hatte im Sommer 2016 ein Bug Bounty Programm gestartet, um Websites des Pentagon auf Schwachstellen zu überprüfen.[34] In Deutschland hat diese Mentalität noch nicht Einzug gehalten, hier gibt es nur wenige größere Unternehmen, die aktiv Bug Bounty Programme betreiben.[35] Der Staat könnte hier leicht Anreize schaffen, indem die Kosten eines Bug Bounty Programms z.B. steuerlich absetzbar wären.

30 Julia Reda. 2016. "European PArliament votes to extend Free Software security audits". https://juliareda.eu/2016/10/ep-votes-to-extend-fossa/

31 GNUPP. 2003. "Zeittafel". http://www.gnupp.de/geschichte.html

32 BSI. 2016. "Verschlüsselung: BSI veröffentlicht Studie zu Open SSL". https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2016/Studie_zu_OpenSSL_02022016.html

33 siehe z.B. https://bugcrowd.com/ oder https://hackerone.com/

34 US Department of Defense. 2016. "Defense Secretary Ash Carter Releases Hack the Pentagon Results". http://www.defense.gov/News/News-Releases/News-Release-View/Article/802929/defense-secretary-ash-carter-releases-hack-the-pentagon-results

35 siehe z.B. Deutsche Telekom. https://www.telekom.com/en/corporate-responsibility/data-protection--data-security/security/security/closing-security-gaps-360054

Fazit

Den DDoS-Attacken der letzten Monate wurde, zu Recht, viel Aufmerksamkeit geschenkt. Währenddessen waren jedoch in Finnland mehrere Häuserblocks ohne Heizung, da die Hausverwaltungsgesellschaft mit einem DDoS-Angriff überfordert war.[36] Und IT-Sicherheitsforscher haben einen Wurm für smarte Glühbirnen entworfen, der sich selbstständig verbreitet und zum Ausfall dieser führen kann.[37] Wenn wir IT-Sicherheit im Internet der Dinge nicht in den Griff kriegen steht daher wesentlich mehr auf dem Spiel als nur ein kurzzeitiger Ausfall populärer Websites.

Daher ist es erfreulich, dass die Bundesregierung in der Cyber-Sicherheitsstrategie 2016 nicht nur über Ausweitung der Produkthaftung nachdenkt, sondern ebenso über Gütesiegel für IT-Sicherheit.[38] Entscheidend ist jedoch, dass es hier keinen nationalen Alleingang gibt und weitere Insellösungen geschaffen werden. Stattdessen sollte die Bundesregierung auf europäischer und internationaler Ebene von Beginn an kooperativ vorgehen, um möglichst viele Unterstützer für solch ein Vorhaben zu gewinnen. Nur dann können entsprechende Mindeststandards und Gütesiegel entsprechende Marktmacht entfalten.

36 Spiegel Online. 2016. “Hacker lassen Finnen frieren”. http://www.spiegel.de/netzwelt/web/finnland-hacker-schalten-heizungen-aus-a-1120234.html

37 Eyal Ronen, et al. 2016. “IoT goes Nuclear: Creating a ZigBee Chain Reaction”. http://iotworm.eyalro.net/

38 BMI. 2016. “Cyber-Sicherheitsstrategie für Deutschland 2016”. http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cybersicherheitsstrategie-2016.pdf?__blob=publicationFile

Stiftung Neue Verantwortung

Think Tank für die Gesellschaft im technologischen Wandel

Neue Technologien verändern Gesellschaft. Dafür brauchen wir rechtzeitig politische Antworten. Die Stiftung Neue Verantwortung ist eine unabhängige Denkfabrik, in der konkrete Ideen für die aktuellen Herausforderungen des technologischen Wandels entstehen. Um Politik mit Vorschlägen zu unterstützen, führen unsere Expertinnen und Experten Wissen aus Wirtschaft, Wissenschaft, Verwaltung und Zivilgesellschaft zusammen und prüfen Ideen radikal.

So erreichen Sie den Autor:

Jan-Peter Kleinhans
jkleinhans@stiftung-nv.de
+49 30 8145 0378 99

Impressum

Stiftung Neue Verantwortung e. V.
Beisheim Center
Berliner Freiheit 2
10785 Berlin
T: +49 (0) 30 81 45 03 78 80

www.stiftung-nv.de
Twitter: @SNV_Berlin

Design:
Make Studio

Layout:
Franziska Wiese