WIEN / 30. April 2019

Stellungnahme für den Ausschuss für Konsumentenschutz

Im Bezug auf den Antrag 102/A(E) betreffend Allgegenwärtige Überwachung im Internet der Dinge auf Kosten des Konsumentenschutzes und Antrag 105/A(E) betreffend Allgegenwärtige Überwachung im Internet der Dinge auf Kosten des Konsumentenschutzes - insbesondere der Smart-Cars

Für epicenter.works
Iwona Laub
Andreas Czák, BSc
Mag.ª Angelika Adensamer, MSc
Thomas Lohninger

EPICENTER .WORKS
for digital rights

Inhaltsverzeichnis

VORWORT

Die Grundrechts-NGO epicenter.works, die sich mit Gesetzen und Regeln im digitalen Raum befasst, sieht beim Gesetzgeber in Sachen KonsumentInnenschutz bei Internet of Things und im Speziellen bei Smart Cars vor allem zwei Hauptanliegen, die auch bereits der Chaos Computer Club (CCC) in seiner Stellungnahme zum deutschen IT-Sicherheitsgesetz[1] erwähnt hat: Die Begrenzung des Schadenpotentials und die Prävention bzw. die Bewusstseinsbildung.

Begrenzung des Schadenpotentials

Der Gesetzgeber hat dafür Sorge zu tragen, Möglichkeiten der Ausnutzung von Systemen einzugrenzen und die Attraktivität von Systemen für Angreifer zu verringern. Zudem muss hier ein Regelwerk geschaffen werden, das die Incentivierung von Unternehmen erhöht, die Sicherheit der Daten ihrer Kundinnen und Kunden zu stärken, da diese oft keine marktwirtschaftlichen Anreize als solche haben. Viele Verteidigungsszenarien stehen den Geschäftsinteressen der Unternehmen direkt entgegen, vor allem wenn es potenzielle Schäden an „Dritten" gibt. Diese finden nur dann ausreichende Berücksichtigung, wenn sie mit einem direkten oder indirekten Geschäftsrisiko einhergehen. Beispiel: „Interne geschäftsrelevante Informationen und Daten unterliegen einem höheren Schutzniveau als KundInnendaten." Wie der CCC weiter schreibt, ist aber genau diese gesellschaftliche Perspektive und Tendenz nicht wünschenswert, weshalb die zweite Aufgabe des KonsumentInnenschutzes zum Einsatz kommt.

Prävention und Bewusstseinsbildung

Es ist Aufgabe des KonsumentInnenschutzes, die Konsumentinnen und Konsumenten aufzuklären, ihnen Information zur Verfügung zu stellen, zu beraten und bestehende Regeln zu evaluieren und weiterzuentwickeln. Das ist besonders wichtig, wenn es Technologien und Software betrifft, die ständig weiterentwickelt wird und deren Einsatzgebiet sich sukzessive erweitert. Die Bewusstseinsbildung ist aber nicht nur bei den Kundinnen und Kunden anzusetzen, sondern auch in kleinen und mittelständischen Unternehmen, da dort die Sensibilität für IT-Sicherheit und die Gefahren des Social Engineerings und das Befolgen von Sicherheitsregeln noch wenig präsent sind.

Konkrete Anforderungen

Allgemein

Hinsichtlich der rasanten Entwicklung internetfähiger Geräte muss ein Framework geschaffen werden, das die Anliegen der Kundinnen und Kunden in den Vordergrund rückt, aber weiterhin gewährleistet, dass Innovation und Unternehmertum möglich sind und gefördert werden. Allgemein kann der Einsatz egal welcher Software, die mit dem Internet verbunden ist, auf Sicherheitsstandards überprüft werden. Der Gesetzgeber kann dafür Sorge tragen, seine eigene zum Einsatz gekommene Software ordentlich zu schützen, indem er a) regelmäßige unabhängige Prüfungen von Open Source Software initiiert bzw. für das Finden und Beseitigen kritischer Sicherheitslücken belohnt und b) indem er die Haftungsfrage für proprietäre Software löst und konkrete Anreize zur Qualitätssicherung verlangt. So

1 https://www.ccc.de/system/uploads/186/original/ITSG_Stellungnahme.pdf

könnten Verschleppungen dieser Maßnahmen mit einer Haftung für den Diensteanbieter im Schadensfall einhergehen. Aus unserer Sicht sind die konkreten Problemstellungen im KonsumentInnenschutz folgende und sollten sich in einem Regelwerk niederschlagen, das Konsumentinnen und Konsumenten Rechtssicherheit bietet.

Interoperabilität

Proprietäre Software von diversen Anbietern muss bis zu einem gewissen Ausmaß eine Interoperabilität ermöglichen, also die Fähigkeit, mit anderen Systemen zusammenzuarbeiten. Beispiel: Ein smarter Toaster, der nur mit einer bestimmten Toastbrot-Sorte zurecht kommt, kann für die Konsumentin und den Konsumenten massive Nachteile bringen. Gerade in der Übertragung der Daten sollte offen gelegt werden, wie diese mit anderen Geräten und/oder dem allgemeinen Teil des Internets kommuniziert wird. Mit diesem Thema befassen sich bereits viele Vertreterinnen und Vertreter aus Wirtschaft, Wissenschaft und Standardisierungskonsortien. Viele der jetzigen Plattformen, auf denen Internet of Things laufen, operieren bereits auf proprietären Systemen und Protokollen, Schnittstellen und miteinander inkompatiblen Standards. Der Mangel an Interoperabilität führt dazu, dass Konsumentinnen und Konsumenten in ein sogenanntes „Vendor Lock-in" fallen, das sie zwingt, ausschließlich Systeme eines bestimmten Herstellers und Diensteanbieters zu nutzen. In einer Studie von McKinsey aus dem Jahr 2018[2] wurde festgestellt, dass allein 40% der Nützlichkeit von Internet of Things Anwendungen und Systemen von der Interoperabilität alleine abhängen. Je besser ein System mit einem anderen kommunizieren kann, desto sinnvoller und nützlicher ist seine Anwendung. Auf wirtschaftlicher Ebene wird in Sachen Interoperabilität mittels Standardisierungen gearbeitet, die nach und nach und mit immer mehr Anwendungen ins Spiel kommen. Auch die Europäische Union hat mit dem Projekt H2020 eine Vision des Verbunds und Zusammenspiels von IoT Plattformen im Visier[3].

Freie Auswahl der Werkstatt/des Händlers oder der Händlerin

Fahrerinnen und Fahrer von Smart Cars sollten die Möglichkeit bekommen, trotz proprietärer Systeme, auf denen diese Art des Fahrens basiert, weiterhin bei mechanischen Schäden eine freie Werkstatt zu wählen. Auch jetzt gibt es Werkstätten, die Autos verschiedener Hersteller analysieren und reparieren können - das muss auch weiterhin möglich sein. Die Anforderungen an diese Betriebe werden selbstverständlich höher werden, denn die Softwarekomponenten dieser Systeme sind mittlerweile komplex. Hier empfiehlt es sich, konkret auf diese Problematik in den Ausbildungsstätten der FahrzeugmechanikerInnen und -elektronikerInnen einzugehen.

Recht auf Offline-Nutzung

Für die Konsumentinnen und Konsumenten stellt sich auch die Frage, inwieweit ein System ohne Internetverbindung noch funktioniert. Es sollte gewährleistet sein, dass auch ohne eine Internetverbindung ein Kühlschrank, ein Toaster oder ein Auto funktionieren müssen. Die Funktionalität eines Geräts darf nicht allein aufgrund seiner Anbindung zum Internet gegeben sein. Es sollte also ein „Recht auf Offline-Nutzung" geben. Beinhaltet so ein Dienst z.B. eine Art Abo-Modell, so muss auch ohne ein Abo die Nutzung in einem bestimmten Rahmen weiterhin möglich sein. Das ferngesteuerte Abdrehen (remote shutdown) sollte nur in absoluten Ausnahmefällen erlaubt sein.

2 Manyika J, Chui M, Bisson P, Woetzel J, Dobbs R, Bughin J, Aharon D (2015) The internet of things: mapping the value beyond the hype. McKinsey global institute. McKinsey Glob Inst 3

3 https://link.springer.com/article/10.1007/s11036-018-1089-9

Recht auf Sicherheit

Der Gesetzgeber sollte sicherstellen, dass der oder die AnbieterIn der Dienste transparent und in weiterer Folge verantwortungsbewusst mit den Daten der Konsumentinnen und Konsumenten umgeht. Vorgeschriebene Sicherheitsupdates oder Patch-Zyklen sollten ebenso stattfinden wie eine zumindest Ende-zu-Ende-verschlüsselte Übertragung von Daten und die Aufschlüsselung aller Daten, die gesammelt und gegebenenfalls an Dritte weitergegeben werden. Gefundene Schwachstellen sollten innerhalb einer bestimmten Zeit beseitigt werden müssen.

Auch muss der Gesetzgeber sicherstellen, dass staatliche Manipulation von Fahrzeugsoftware aufgrund der drastischen möglichen Auswirkungen auf die Verkehrssicherheit nicht geschieht. Das legitime staatliche Interesse an Überwachung muss in den Hintergrund treten wenn das Risiko besteht, dass durch herstellerfremde Eingriffe Auswirkungen auf Lenkung, Beschleunigung Bremsen oder ähnlichem auftreten können. Es gibt viele Möglichkeiten Fahrzeuge zu überwachen, eine Spionage durch das Fahrzeug selbst ist aufgrund obiger Bedenken abzulehnen. Jede Sicherheitslücke, die dem Staat offen steht, um Überwachung zu betreiben, steht auch Kriminellen offen.

Recht auf Datenschutz

Die Konsumentinnen und Konsumenten sollten jederzeit die Möglichkeit haben, genau in Erfahrung zu bringen, welche Daten zu welchem Zeitpunkt und zu welchem Zweck verschickt, gespeichert und verarbeitet werden. Das Teilen von teilweise sensiblen personenbezogenen Informationen zum Nutzungsverhalten verschiedener Geräte - insbesondere von Smart Cars - sollte nur dann stattfinden, wenn dies für die Nutzung und Optimierung eines Dienstes unbedingt notwendig ist. Auch eine Deklarierung dessen, wo diese Daten genau liegen, sollte ein Anliegen im KonsumentInnenschutz sein. Die Nivellierung an datenschutzrechtlich schlechter gestellte Regionen der Welt ist und kann nicht das Ziel sein, um österreichischen Konsumentinnen und Konsumenten ein sicheres und vertrauenswürdiges Erlebnis mit Internet of Things zu ermöglichen.

Spezifisch beim eCall lautet unsere Forderung, dass das eCall System solange offline ist, bis ein Schadensfall oder aktiver Notruf abgesetzt wird. Keinesfalls soll das System dauerhaft aktiviert sein um so lückenloses Tracking von einzelnen AutofahrerInnen zu ermöglichen.

Konkurs/Geschäftsauflösung

Im Fall einer Geschäftsauflösung eines Dienstanbieters sollten Konsumentinnen und Konsumenten vom Unternehmen proaktiv informiert werden müssen, wie es mit der Sicherheit der Software weitergeht und inwiefern das die Nutzung des Geräts beeinflussen wird. Vorstellbar wäre beispielsweise die Verpflichtung, Software Escrow Services zum Einsatz kommen zu lassen. Das sind Dienste, die nach der Geschäftsauflösung eines Unternehmens die Software weiter betreiben und Sicherheitsupdates ausspielen.

Mindeststandards und Kennzeichnungspflicht

Ähnlich dem CE Siegel für Geräte, die unter Maßgabe von Sicherheitsanforderungen an das Stromnetz angeschlossen werden können, sollten auch Geräte, die am offenen Internet betrieben werden, gewissen Mindeststandards genügen müssen. Die Mindestanforderungen für ein solches verpflichtendes Gütesiegel sollten unter Einbeziehung der Gerätehersteller, unabhängiger Sicherheitsforscherinnen und -forschern und staatlicher Stellen festgelegt werden. Daran anschließend fordern wir eine Kennzeichnungspflicht aller neu verkauften Geräte mit Internetanschluss, wie lange diese vom Hersteller mit Sicherheitsupdates versorgt werden. Es ist bis

heute möglich, dass auch Geräte bereits wenige Wochen nach dem Kauf keine Sicherheitsupdates mehr bekommen und damit für eine sichere Verwendung für Anwendungen wie Netbanking unbrauchbar sind. Sicherheitsupdates sollte für diesen Zweck von regulären Updates zur Erweiterung des Funktionsumfangs getrennt werden.

Geplante Obsoleszenz

Wie auch bei nicht-internetfähigen Geräten, sollte die Vermeidung von geplanter Obsoleszenz ein zentraler Aspekt in der Etablierung des KonsumentInnenschutzes von Internet of Things sein. Die Funktionsfähigkeit und Sicherheit eines Systems sollte nicht künstlich verschlechtert werden, um Konsumentinnen und Konsumenten zur Erneuerung zu zwingen. Die Obsoleszenz sollte in einem akzeptablen Rahmen bleiben, der unter Berücksichtigung softwaretechnischer, mechanischer und rechtlicher Argumente ausgelegt sein soll. Gerade auch die finanzielle Frage ist mit der geplanten Obsoleszenz wichtig. Aufgrund immer größerer Armut in Österreich, kann von der Bevölkerung nicht abverlangt werden, immer am allerneuesten Stand der Technik zu sein. Auch "ältere" Modelle aus vorigen Generationen bestimmter Geräte müssen den Sicherheitsstandards entsprechen und leistungsfähig sein.

Bewusstseinsbildung und Prävention

Die technologische Entwicklung ist unaufhaltsam und sehr rasch, weshalb es unwahrscheinlich ist, dass die Gesetzgebung in der selben Dynamik und Zeit auf entsprechende Änderungen reagieren kann. Darum ist eine der zentralen Anliegen im KonsumentInnenschutz die Bewusstseinsbildung und damit einhergehende Prävention von Schadensfällen. Die Bevölkerung muss besser auf diesen Wandel vorbereitet werden, um in der Gesellschaft ein besseres Gespür und Bewusstsein dafür zu etablieren, vorsichtig mit Daten und mit dem Internet verbundene Geräte umzugehen.

Im Schadensfall

Sollten Daten von Konsumentinnen und Konsumenten in die Hände Unbefugter gelangen - auf welchem Weg auch immer - sollte das Informieren der Nutzer sowie deren Re-Identifikation und darauffolgende Änderung der Zugangsdaten ein absolutes Muss sein. Die Verpflichtung zur Information bei Verletzung des Datenschutzes besteht bereits nach der DSGVO. Den Kundinnen und Kunden muss ein Mindestmaß an Transparenz gewährleistet werden, um im Falle des Falles den Schaden maximal zu minimieren.

CONCLUSIO – QUALITÄT DURCH REGULIERUNG

In Anbetracht dessen, dass Konsumentinnen und Konsumenten naturgemäß einerseits nicht über ausreichendes technisches Wissen verfügen, um alleine Risikoentscheidungen zu treffen, die von der Sicherheit ihrer IoT Geräte abhängen, andererseits auch bei ausreichendem Wissen vielleicht nicht ausreichend sichere und leistbare Alternativen am Markt vorfinden, lassen sich die oben angeführten Probleme nur durch eine Regulierung von verpflichtenden Qualitätsstandards für alle IoT-Geräte lösen. Wir empfehlen daher, noch bevor die ersten Sicherheitsprobleme auftreten, ein robustes Regelwerk zu Normierung von IoT-Geräten zu schaffen. Dies wird auch dazu dienen, den lokalen Wirtschaftsstandort zu stärken.