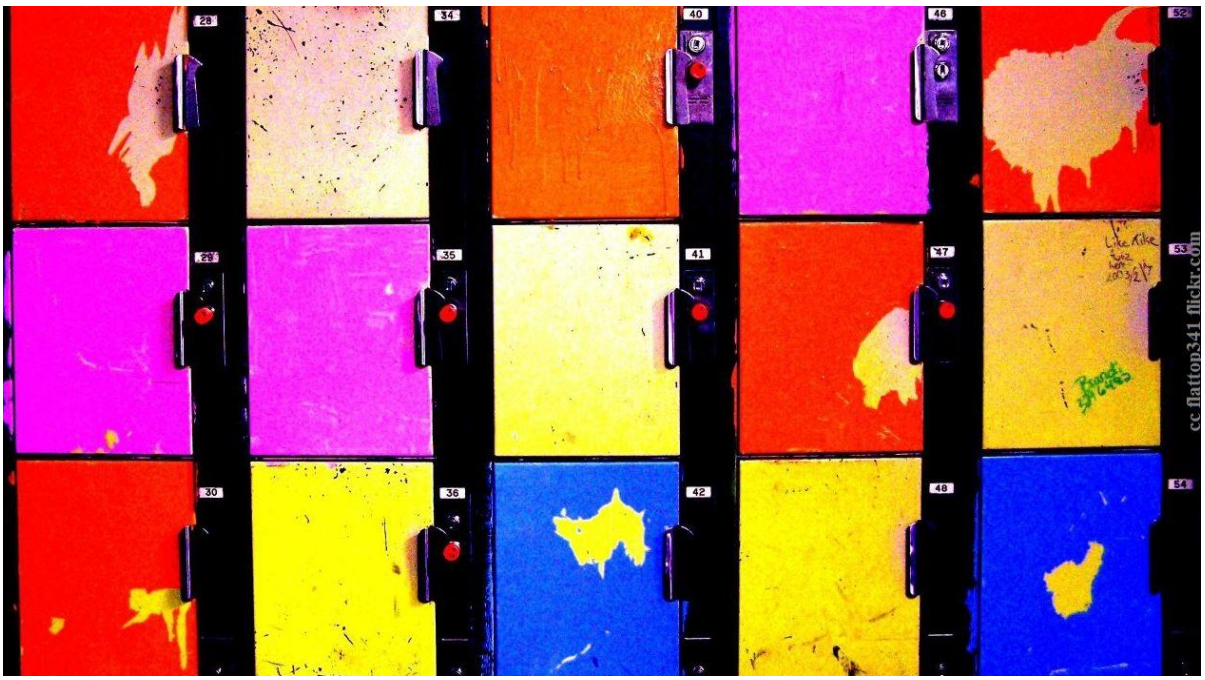
JACQUES DELORS INSTITUT
BERLIN

BLOG POST 07.07.2017

EU und die Sicherheit im Internet der Dinge: Better Safe than Sorry

Paul-Jasper Dittrich
Wissenschaftler beim Jacques Delors Institut – Berlin



Nach jedem Cyberangriff wird der Ruf nach mehr Sicherheit und politischem Eingreifen lauter, auf nationaler oder gleich auf europäischer Ebene. Dabei geht in der Debatte manchmal unter, welcher Natur die unterschiedlichen Angriffe sind und welche regulatorischen und politischen Antworten auf welcher Ebene nötig sind, um diese einzudämmen. In diesem Blog Post erklärt Paul-Jasper Dittrich die Debatte über Cybersicherheit in der EU, zeigt mögliche Handelsfelder für europäische Lösungen auf und erläutert, welche regulatorischen Maßnahmen dazu geeignet sind, Produktsicherheit im Internet der Dinge zu gewährleisten.

Pariser Platz 6
D – 10117 Berlin
Tel.: +49 (0)30 467 26 09 – 01

Online: delorsinstitut.de
E-Mail: office@delorsinstitut.de
Twitter: @delorsinstitut

1 Cyberattacken kennen keine Grenzen

Von den globalen Cybervorfällen und Hackerattacken in den letzten Monaten waren auch europäische Mitgliedstaaten stark betroffen. Diese Angriffe haben schwere ökonomische Schäden hervorgerufen und in einigen Fällen wie dem „WannaCry"-Schadprogramm im Mai 2017 sogar Menschenleben in Gefahr gebracht, weil zum Beispiel Krankenhäuser zum Ziel der Attacken wurden. Diese Angriffe führen uns vor Augen: Bei der Cybersicherheit muss in Europa schneller und beherzter gehandelt werden, auch mithilfe europäischer Regulierung für den Binnenmarkt. Über die konkrete Rolle der EU gehen die Meinungen allerdings auseinander.

Denn einerseits braucht es bei der Cybersicherheit mehr und schnellere europäische Lösungen: Nur wenn der ganze europäische Binnenmarkt besser gegen Hackerattacken und Cyber-Erpressungsversuche (Ransomware) abgeschirmt wird, werden europäische Endverbraucher genug Vertrauen in die gerade aufkommenden vernetzten Geräte des Internets der Dinge bekommen. Dazu kommt der direkte, wirtschaftliche Schaden durch Hackerattacken, den der Branchenverband Bitkom allein für die deutsche Wirtschaft auf 51 Milliarden Euro pro Jahr beziffert.

Andererseits werden trotz Einigkeit und erhöhter europäischer Kooperation (z.B. bei der Forschung und beim Informationsaustausch) von den Regierungen der Mitgliedstaaten oft Subsidiaritätsvorbehalte geäußert. Das gilt insbesondere dort, wo der Schutz der nationalen kritischen Infrastruktur betroffen ist oder es um Maßnahmen gegen den Zugriff fremder Mächte auf sensible Informationen oder gar Staatsgeheimnisse geht. Das bedeutet aber nicht, dass der EU nicht trotzdem eine sehr wichtige Rolle dabei zukommt, den gemeinsamen Binnenmarkt besser vor Cyberattacken zu schützen.

Dabei fällt auf, dass die Debatten um IT- und Produktsicherheit oft stark mit Diskursen wie dem Schutz kritischer Infrastruktur oder der Abwehr fremder Mächte im Cyberspace vermischt werden. Während IT- und Produktsicherheit vor allem ein wirtschaftliches Politik- und Regulierungsfeld ist, spielen beim Schutz der Infrastruktur und staatlichen Hackerangriffen auch sicherheits- und außenpolitische Erwägungen eine Rolle.

Welche Cybersicherheit?

Von welcher Sicherheit ist dann genau die Rede, wenn von Cybersicherheit gesprochen wird? Cyberattacken können äußerst unterschiedliche Ziele verfolgen und dabei auf ganz verschiedene Wege und unter Einsatz unterschiedlichster technischer Mittel ihr Ziel erreichen: Die Attacke

auf den amerikanischen DSN-Provider Dyn im Oktober 2016 erfolgte zum Beispiel über hunderttausende mit dem Internet verbundene Alltagsgegenstände wie Überwachungskameras, Router oder Waschmaschinen. All diese miteinander vernetzten Geräte aus dem Internet der Dinge wurden von einem Botnetz übernommen und stellten zeitgleich Anfragen an die Server des Internetdienstleisters, die wegen Überlastung zusammenbrachen. Die Folge waren Seitenausfälle bei hunderten amerikanischen Unternehmen, die auf die Dienste von Dyn zurückgreifen, darunter Twitter und Amazon, deren Seiten über Stunden nicht erreichbar waren. Andere Attacken, wie die beiden letzten Ransomware-Attacken mit der „Wannacry“ oder „Petya“-Malware sprangen über eine Sicherheitslücke in Windows XP von Computer zu Computer. Wiederum ganz anders gelagert war der Fall der russischen Hacker, die im Jahr 2015 Daten von den Servern des Bundestags mithilfe einer Phising-Mail und eines Links zu einem Schadprogramm erbeuteten.

Eines haben diese Fälle allerdings gemein: Nach dem Bekanntwerden eines Angriffs wird jedes Mal der Ruf nach mehr Cybersicherheit und politischem Eingreifen lauter, entweder auf nationaler oder gleich auf europäischer Ebene. Dabei geht in der Debatte manchmal unter, welcher Natur die unterschiedlichen Angriffe sind und welche regulatorischen und politischen Antworten auf welcher Ebene nötig sind, um diese einzudämmen. Im Falle eines Angriffs wie auf den Internetdienstleister Dyn steht vor allem Produktsicherheit im Vordergrund, also die Frage, wie Produkte im Internet der Dinge gegen Übernahme in Botnetze sicher gemacht werden können. Angriffe auf die kritische Infrastruktur mithilfe von Malware, wie in der letzten Zeit häufig in der Ukraine geschehen, brauchen eine Stärkung der nationalen Abwehrfähigkeiten, beispielsweise durch ein nationales Cyberabwehrzentrum. Angriffe wie der auf den Bundestag hingegen, verlangen eine politische, diplomatische und eventuell geheimdienstliche Antwort sowie Schulungsmaßnahmen, um Mitarbeiter noch stärker für derartige Bedrohungen zu sensibilisieren. Es wird deutlich: Cybersicherheit kann es nur dann geben, wenn die vielschichtigen Bedrohungen auf allen Ebenen individuell und konkret adressiert werden.

2 Warum Toaster sicher vor Angriffen sein müssen

Hier kommen die EU und das europäische Mehrebensystem ins Spiel: Worin besteht der europäische Mehrwert bei der Cybersicherheit? Im Moment sieht es danach aus, dass vor allem bei der Frage der Produkt- und IT-Sicherheit im Internet der Dinge schnell eine europäische Lösung gefunden werden könnte und sollte. Das hat zum einen den Grund, dass die fehlende Produktsicherheit einen Fall von Marktversagen darstellt und die EU damit einen Regulierungsauftrag im Binnenmarkt begründen kann. Individuelle nationale Lösungen würden hier letztendlich eine europäische Verordnung oder Richtlinie unnötig herauszögern: Es bestünde dann wieder einmal ein Flickenteppich, der mühsam vereinheitlicht werden müsste. Zum anderen ist Produktsicherheit das einzige Politikfeld, bei dem die Subsidiaritätsbedenken

vergleichsweise niedrig sind. Der Schutz kritischer Infrastruktur und die Cyberabwehr fremder Mächte wird in den meisten europäischen Hauptstädten weiterhin als nationale Kompetenz und als eine Aufgabe gesehen, bei der die nationalen Administrationen in naher Zukunft wenig bis gar keine Handlungssouveränität an die europäische Ebene abgegeben möchten. Zwar schreibt die 2016 verabschiedete NIS-Richtlinie stärkere Kooperation zwischen den europäischen Regierungen vor und etabliert beispielsweise Meldepflichten über Vorfälle und mehr Befugnisse für die europäische Cyber-Agentur ENISA. Bei der konkreten Hilfe zur Abwehr von Bedrohungen verlassen sich aber nationale Unternehmen in der Regel weiterhin auf ihre „eigene" Regierung. Dies gilt auch, wenn sich der Vorfall auf dem Staatsgebiet eines anderen EU-Mitglieds ereignet hat (beispielsweise innerhalb einer integrierten Produktionskette). Insofern schreibt die NIS-Richtlinie zwar den einzelnen EU-Staaten vor, ihre eigene kritische Infrastruktur zu schützen und dafür entsprechende Cyber-Strategien zu entwickeln und mit den europäischen Partnern im konstanten Informationsaustausch zu bleiben. Die aufgebauten Kompetenzen bleiben allerdings vorerst mehrheitlich auf nationaler Ebene und werden nicht europäisch gebündelt. Produktsicherheit im Internet der Dinge hingegen ist ein klassisches Binnenmarktthema.

Fehlende Sicherheit ist eine negative Externalität

Ökonomisch gesehen handelt es sich bei der fehlenden IT-Sicherheit im Internet der Dinge um eine negativen externen Effekt. Sowohl Produzenten als auch Konsumenten von mit dem Internet verbundenen Geräten haben in der Regel keinen direkten Nachteil davon, wenn ihr Gerät gehackt und beispielsweise Teil eines Bot-Netzes wird. Daher stecken Produzenten kein Geld in (kostspielige) Sicherheitsfeatures und Updates und Konsumenten fordern diese auch nicht nachdrücklich von Produzenten ein. Das Resultat dieser fehlenden Anreize auf beiden Seiten ist im Aggregat fehlende IT-Sicherheit sowie ein Schaden für die Wirtschaft und Gesellschaft im Ganzen durch Hackerangriffe. Ähnlich wie bei der Umweltverschmutzung leiden nicht unmittelbar konkrete Konsumenten oder Produzenten, sondern die ganze Gesellschaft.

Bei solchen negativen externen Effekten kann die EU gutbegründet marktregulierend eingreifen. Die Produktsicherheit und IT-Sicherheit für das Internet der Dinge sollte also so schnell wie möglich angegangen werden. Anderenfalls drohen schon in naher Zukunft wirtschaftliche Einbußen. Denn in den nächsten Jahren werden Milliarden vernetzter Geräte für Endverbraucher auf den Markt kommen, bis in nicht ganz allzu ferne Zukunft fast jeder Haushaltsgegenstand eine Internetverbindung haben könnte. Diese Entwicklung wird für Europa aber nur dann ein Erfolg, wenn absolut klar ist, dass die Geräte sicher sind und nicht zum Nachteil der Gesellschaft von Kriminellen oder gar feindlichen Mächten gekapert werden können.

3 Ist Produkthaftung die Lösung?

Die EU hat viele Instrumente in ihrem Baukasten zur positiven Integration durch Marktregulierung. Welche sind am sinnvollsten, um eine möglichst hohe Produktsicherheit im Internet der Dinge zu gewährleisten? Eine Übersicht über die wichtigsten regulatorischen Instrumente hat Jan-Peter Kleinhans von der Stiftung Neue Verantwortung aufgestellt. So könnte die EU beispielsweise von den Produzenten einheitliche Standards verlangen, Labels einführen, eine Produzentenhaftung beziehungsweise Produkthaftung für Konsumgeräte im Internet der Dinge etablieren oder auf freiwillige Selbstkontrolle der Produzenten setzen. Im medialen Diskurs spielt vor allem die Produzentenhaftung immer wieder eine große Rolle. Eine solche Haftung würde darauf hinauslaufen, dass die Produzenten von internetfähigen Geräten für durch Cyberattacken entstandene Schäden haften. Während aber vor allem in Deutschland nach jedem neuen Cybervorfall die schnelle Einführung der Produkthaftung gefordert wird, herrscht unter Experten Uneinigkeit, ob eine rasche Einführung einer solchen Herstellerhaftung durchführbar und überhaupt zweckdienlich und wünschenswert ist. Zu viele Fragen sind nämlich noch ungeklärt, da es sich beim Internet der Dinge um eine ganz neue Kategorie von Produkten handelt. So ist beispielsweise unklar, wie mit Geräten umgegangen werden soll, die Open Source-Software verwenden, wie der letztendlich haftende „Produzent" bestimmt werden kann (ist es der Hardware- oder Softwarehersteller oder der Distributor der Produkte?) oder wie mit Geräten umgegangen werden soll, bei denen die Produzenten längst vom Markt verschwunden sind, deren Produkte aber weiterhin Updates benötigen.

Sinnvoller wäre eine Einführung von Mindeststandards europaweit und erst danach eventuell eine Ausweitung der Haftung auf die Hersteller von Produkten im Internet der Dinge. In jedem Falle sollte die EU-Kommission bei diesem Thema das Heft nicht aus der Hand geben, um von Beginn an eine einheitliche Lösung für den gemeinsamen Markt zu schaffen. Damit wäre ein wichtiger Baustein realisiert, um das Potential des Internets der Dinge in der EU voll auszuschöpfen.