Die großen deutschen Mobilfunkunternehmen bereiten sich bei ihren Planungen für den neuen Mobilfunkstandard 5G bereits auf einen teilweisen Boykott des chinesischen Ausrüsters Huawei vor. Offenbar hat die Bundesregierung dem Druck der USA nicht standgehalten. Begründet wird dies mit „Sicherheitsbedenken". Das ist interessant, da es bislang keinen Beleg dafür gibt, dass chinesische Dienste Technik von Huawei kompromittiert hätten. Ganz anders als die amerikanischen Konkurrenten, die bereits mehrfach durch NSA-Hintertüren aufgefallen sind. Einen Lichtblick stellt da das Gegenangebot der deutschen Mobilfunknetzbetreiber dar. Doch leider ist es unwahrscheinlich, dass die Bundesregierung die Interessen ihrer Bürger und Unternehmen über die Interessen der USA stellt. Von **Jens Berger**.

Dieser Beitrag ist auch als Audio-Podcast verfügbar.

http://www.nachdenkseiten.de/upload/podcast/190205_Juniorpartner_der_USA_im_Handelskrieg_gegen_Huawei_NDS.mp3

Podcast: Play in new window | Download

Seit der chinesische Technikriese Huawei auf dem internationalen Markt tätig ist, wird er von den USA und den Ländern, die zusammen mit den Amerikanern das Geheimdienst-Netzwerk der „Five Eyes" bilden, mit aller Macht bekämpft. Zunächst hinderte man das chinesische Unternehmen daran, westliche Firmen zu übernehmen (z.B. Marconi (GB), 3Com (USA) oder 3Leaf (USA)) und schloss dann Huawei und den chinesischen Mitbewerber ZTE sogar generell bei Ausschreibungen aus – z.B. Sprint (2012/USA) oder NBN (2012/Australien). Nachdem in den letzten Jahren ein wenig Ruhe in den Handelskrieg gegen Huawei einkehrte, entfachte Donald Trump den Konflikt mit seiner zur Außenhandelsdoktrin erhobenen „America-First-Strategie" neu und erklärte China den Handelskrieg.

Seitdem ist Huawei in den USA, Japan, Taiwan, Australien und Neuseeland beim Aufbau des 5G-Netzes offiziell ausgeschlossen. Kanada und Großbritannien prüfen ebenfalls einen Ausschluss – der britische Telekommunikationsgigant British Telecom hat seinerseits bereits erklärt, Huawei freiwillig bei den kommenden 5G-Ausschreibungen auszuschließen. Seit letzter Woche hat die US-Regierung offenbar hinter den Kulissen noch einmal den Ton verschärft und übt nun Medienberichten zufolge massiven Druck vor allem auf Deutschland, Polen und Großbritannien aus. Deutschland scheint dabei – wie gewohnt – als erstes einzuknicken und stellte bereits vor zwei Wochen Huawei öffentlich „als 5G-Ausrüster in Frage", stößt dabei jedoch bis dato bei den Mobilfunknetzbetreibern auf Widerstand, die

Huawei als zuverlässigen und preiswerten Ausrüster schätzen.

Um was geht es eigentlich bei diesem Handelskrieg? Offiziell ist beim Vorgehen gegen Huawei und den zweiten chinesischen Anbieter ZTE immer wieder von „Sicherheitsproblemen" die Rede. Es handele sich schließlich um ein chinesisches Unternehmen und China sei ja bekannt dafür, auch mittels IT-Technik Spionage und Industriespionage zu betreiben. Ein Einfallstor für fremde Dienste mitten im technischen Rückgrat der Zukunftstechnologie Nummer Eins in der Kommunikationstechnik wäre freilich ein großes Problem. Und dass China – so wie jede größere Nation – aktiv Spionage betreibt und chinesische Unternehmen Industriespionage betreiben, ist bekannt. **Für die stets behauptete Kompromittierung der Produkte von Huawei durch chinesische Dienste gibt es jedoch keinen Beleg**. Im Gegenteil. Bereits 2012 hatte Huawei den australischen Behörden gegenüber angeboten, den – eigentlich streng geheimen – Quellcode, der in den Huawei-Produkten genutzten Firm- und Software offenzulegen. Dieses Angebot wiederholte Huawei immer wieder – auch aktuell steht ein Angebot an das Bundesamt für Sicherheit in der Informationstechnologie (BSI) im Raum.

Deutsche Behörden könnten sich an dieser Stelle auch ganz einfach an heimische Forschungseinrichtungen wenden. Huawei hat zwar seinen Sitz in China, ist aber in der Forschungs- und Entwicklungsarbeit in Deutschland sehr aktiv. So wurde beispielsweise die 5G-Technik, die nun im Mittelpunkt des Handelskrieges steht, von Huawei zusammen mit der TU München in einem Testprojekt erprobt, das von der Bayerischen Staatsregierung und der Stadt München mitfinanziert wurde. Huawei forscht in Sachen 5G auch zusammen mit dem Fraunhofer Institut, der RWTH Aachen, der Humboldt-Universität Berlin und 240 weiteren Forschungs- und Kooperationsprojekten mit europäischen Universitäten, Instituten und Unternehmen. Huawei beschäftigt in der EU rund 10.000 Mitarbeiter, wobei jeder vierte von ihnen einen hochqualifizierten Job im Bereich Forschung und Entwicklung hat. Das Unternehmen ist also keinesfalls ein „schwarzes intransparentes Loch", wie es vor allem die US-Propaganda gerne suggeriert.

Wie sieht es eigentlich bei der Konkurrenz von Huawei in Sachen Transparenz und Sicherheit aus? Im Netzwerkbereich sind die großen Konkurrenten von Huawei in der Tat spätestens seit den Snowden-Enthüllungen vor allem für ihre „Sicherheitsprobleme" im Zusammenhang mit den US-Geheimdiensten bekannt. Branchen-Primus Juniper Networks hatte beispielsweise jahrelang einen „Zufallsgenerator" in seiner Betriebssoftware, dessen zufällige Zahlen nicht wirklich zufällig waren und von der NSA vergleichsweise einfach erraten werden konnten – dadurch konnte die NSA beispielsweise „verschlüsselte" Kommunikation über VPN-Netzwerke mitlesen, die vor allem in sicherheitsrelevanten Bereichen in der Unternehmenskommunikation Standard sind. Nicht der Hersteller oder

eine Behörde haben diese Hintertür entdeckt, die offenbar seit 2008 offenstand und von Juniper-Entwicklern eingebaut wurde, sondern Hacker und erst Snowdens Enthüllungen konnten den Druck auf Juniper Networks aufbauen, diese Hintertür langsam und allmählich zu schließen. Ob und welche Hintertüren die NSA in die aktuellen Produkte des Unternehmens aus Sunnyvale/Kalifornien eingebaut hat, ist unbekannt. Es ist aber unwahrscheinlich, dass zur Zeit keine derartigen Hintertüren der NSA implementiert sind.

Das gilt auch für Cisco Systems aus San José/Kalifornien. Hier schafften es erst die Hacker von „Shadow Broker", eine jahrelang existente Hintertür der NSA offenzulegen. Mittlerweile gilt der Marktführer aus den USA als derart unsicher, dass sicherheitssensitive deutsche Unternehmen und Forschungseinrichtungen, wie das Deutsche Zentrum für Luft- und Raumfahrt, Cisco-Produkte ausmustern und gegen heimische Alternativen ersetzen. Das mag auf Firmenebene auch möglich sein – wenn man bedenkt, dass alleine Cisco auf dem Switching- und Routermarkt einen Weltmarktanteil von mehr als 50% hat, ahnt man bereits, wie schwer ein großflächiger Ersatz sein dürfte. In Spezialbereichen sind Alternativen ohnehin Mangelware. **Leider muss man daher feststellen, dass ein Großteil des technischen Rückgrats des Internet und der großen Firmennetzwerke aus Technik besteht, auf die US-Dienste wie die NSA wahrscheinlich über Hintertüren und Zweitschlüssel weitreichenden Zugriff haben.** Das mag die Bundesregierung in ihrer berüchtigten Nibelungentreue zu den USA ja unproblematisch finden – deutsche Firmen und Forschungseinrichtungen und nicht zuletzt die deutschen Bürger sehen das hingegen ein wenig anders.

Also lieber die chinesische Technik, von der man nicht weiß, ob und wie viel sie ausspioniert, als die US-Technik, von der man sehr sicher annehmen muss, dass sie aktiv von der NSA kompromittiert ist? **Nein, es muss einen dritten Weg geben.** Und diesen dritten Weg schlägt in der aktuellen Debatte die Deutsche Telekom vor, die von einem Huawei-Boykott besonders hart betroffen wäre. Die Telekom schlägt – offenbar in Absprache mit den Konkurrenten Vodafone und Telefonica – vor, die in den großen deutschen Netzwerken zugelassene Technik generell einer Zertifizierung durch unabhängige Prüflabors wie das BSI zu unterwerfen und die Hersteller dabei sogar zu zwingen, den Quellcode ihrer Software offenzulegen. Offene Quellcodes (Open Source) sind keinesfalls ungewöhnlich und werden – z.B. beim Betriebssystem Linux – mit großem Erfolg eingesetzt. Ein Großteil der genutzten Software, die auf Servern läuft, ist ohnehin quelloffen – das gilt jedoch nicht für die Firmware der in den Servern genutzten Hardwarekomponenten und die Software, die auf den externen Komponenten wie Switches und Router läuft.

Würde Deutschland diesen Vorschlag umsetzen und proprietäre Software – also

Software mit Code, der nicht öffentlich zugänglich ist – in der Netzwerktechnik, die das Rückgrat des kommenden 5G-Netzes bildet, verbieten, wäre dies ein riesiger Schritt in Sachen Transparenz und Sicherheit. Huawei hat – als einer der wenigen Hersteller in dieser Branche – ja bereits von sich aus angeboten, seine Quellcodes offenzulegen. Ob Cisco, Juniper, HP und ihre europäischen Mitbewerber Nokia und Ericson diesem Beispiel folgen würden, ist indes offen. Gar keinen Gefallen an diesem Vorschlag dürften die NSA, das britische GCHQ und vielleicht ja auch die chinesischen Dienste haben. Daher kann es auch nicht überraschen, dass das Bundeswirtschaftsministerium den Vorschlag von Telekom und Co. „noch nicht „kommentieren will“ – hinter den Kulissen werden die USA momentan mächtig Druck machen. Leider ist es unwahrscheinlich, dass die Bundesregierung die Interessen ihrer Bürger und die Interessen der deutschen Wirtschaft im Konfliktfall über die Interessen der USA stellt. Wahrscheinlicher ist es da, dass man der Order des großen Bruders einmal mehr folgt und den chinesischen Ausrüster bei den Ausschreibungen für das 5G-Netz ausschließt; auf dass uns die NSA auch weiterhin bespitzeln kann.

Titelbild: Ink Drop/shutterstock.com