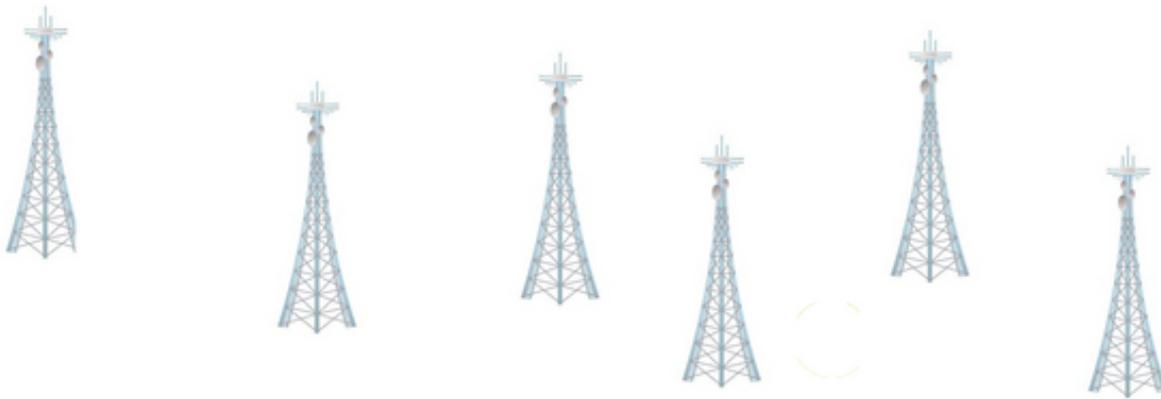


Die Angst vorm Abhören

Der chinesische Konzern Huawei will in Europa das schnelle 5G-Mobilnetz aufbauen. Doch nicht alle fühlen sich damit besonders wohl. Vielleicht sogar aus gutem Grund.

Von Claudia Zettel



Ein Gespenst geht um in der Mobilfunkwelt: Es trägt den Namen Huawei. Im Zuge des Auf- und Ausbaus der 5G-Netze ist auch eine Diskussion darüber entbrannt, wie sehr man dem chinesischen Konzern vertrauen kann. Huawei ist einer der weltweit führenden Anbieter für die benötigte Netzwerkinfrastruktur. Doch insbesondere die USA werfen dem Konzern eine große Nähe zur chinesischen Regierung vor und fürchten Spionageaktivitäten und Sabotage. Infolge sind auch in der EU Zweifel aufgekommen, ob man ausgerechnet auf Huawei setzen sollte, wenn es um die nächste Mobilfunkgeneration geht. Doch endgültige und klar ausformulierte Standpunkte gibt es bislang nicht.

Im Herbst vergangenen Jahres warnte die EU-Kommission vor Gefahren durch 5G-Anbieter außerhalb der Europäischen Union. Unternehmen könnten versuchen, durch den Diebstahl geistigen Eigentums Wettbewerbsvorteile zu erlangen, hieß es in einem Bericht, den die Brüsseler Behörde im Oktober vorstellte. Die Gefahr könne von Staaten sowie von staatlich unterstützten Akteuren ausgehen, so die Sorge. Vor allem Letztere könnten die „Motivation, Absicht und Fähigkeit haben, anhaltende und ausgefeilte Angriffe“ auf 5G-Netze durchzuführen, las man in dem Bericht. Die Motivation solcher Angriffe sei hauptsächlich politisch. Die EU-Kommission nannte den chinesischen Anbieter Huawei in diesem Zusammenhang zwar nicht namentlich, spielte aber durchaus indirekt auf ihn an.

An einer anderen Stelle des Berichts hieß es weiter: Huawei, Ericsson, und Nokia seien im Hinblick auf den Marktanteil die Hauptakteure im 5GBereich, weitere seien ZTE, Samsung und Cisco. Ericsson und Nokia hätten ihre Hauptquartiere in der EU, die anderen jedoch nicht. „Ihre Unternehmensführung weist erhebliche Unterschiede auf, etwa mit Blick auf das Level an Transparenz und die Eigentumsverhältnisse der Unternehmen.“ Auch der EU-Rat warnte indirekt vor Huawei. So wurde im November vergangenen Jahres ein Beschluss vorgelegt, der bestimmte Regelungen für den 5G-Ausbau vorschlägt. Darin wird vor den „rechtlichen und politischen“ Rahmenbedingungen für Anbieter aus Drittstaaten gewarnt. Es müsse in besonderem Maße auf die Risikoprofile einzelner Anbieter geachtet werden. Befürchtet wird seitens EU-Vertreterinnen und -Vertretern außerdem, dass man sich von einzelnen Anbietern abhängig machen könnte.

Die Politik hält sich zurück – aus gutem Grund

Auf politischer Ebene ging auch zu Beginn des neuen Jahres der Seiltanz um die Positionierung zu Huawei weiter. Deutschland beispielsweise hat sich bisher ebenso wenig festgelegt, ob es Huawei vom Netzausbau ausschließen wird oder nicht, wie Österreich. Einerseits teilt man die weit verbreiteten Bedenken bezüglich der Vertrauenswürdigkeit des chinesischen Konzerns, andererseits weiß man auch um die möglichen Folgen, käme es tatsächlich so weit. So hat China bereits angedeutet, dass es Konsequenzen für Deutschland haben werde, sollte Huawei vom deutschen Markt ausgeschlossen werden. Die Drohgebärde kam zum Beispiel seitens der chinesischen Botschaft in Berlin und ging dabei in Richtung der deutschen Autoindustrie in China.

Zuletzt zögerte auch die deutsche Bundeskanzlerin Angela Merkel eine klare Aussage erneut hinaus. Vor März 2020 ist nun jedenfalls keine Entscheidung in der Huawei-Frage zu erwarten. Auch die österreichische Landwirtschaftsministerin Elisabeth Köstinger, zu deren Agenden nun auch 5G und Breitband gewandert sind, legte sich bislang nicht fest. Der Status quo lautet: Man werde sich alles ganz genau anschauen. Österreichs Bundeskanzler Sebastian Kurz betonte unlängst, dass man technologieneutral agieren und gleichzeitig ein Maximum an Sicherheit haben wolle. Bei der Frage, ob man Huawei akzeptieren oder ausschließen soll, hofft Kurz auf eine einheitliche europäische Vorgehensweise.

Dass man sich seitens der Politik nur schrittweise an eine Entscheidung herantastet, ist aus Sicht von Expertinnen und Experten nicht ganz unbegründet. „Nach der derzeitigen Rechtslage steht es einzelnen Mitgliedstaaten der EU bzw. der EU als solcher frei, Unternehmen aus Drittstaaten von öffentlichen Auftragsvergaben auszuschließen“, sagt Franz Leidenmühler, Institutsvorstand am Institut für Europarecht an der Johannes Kepler Universität Linz. Die Regelungen für das Auftragswesen würden nur innerhalb der EU gelten, in der Praxis würden oft auch Aufträge nur für EU-Unternehmen ausgeschrieben. „Aus rechts- und vor allem wirtschaftspolitischer Sicht ist aber natürlich bei dem deklarierten Ausschluss eines Unternehmens aus einem Drittstaat mit entsprechenden Gegenmaßnahmen des Herkunftsstaates dieses Unternehmens zu rechnen“, sagt Leidenmühler. „Etwa, dass China als sogenannte Retorsion auch EU-Unternehmen von Auftragsvergaben ausschließt.“ Die Einschätzung des Experten bestätigt also genau das, was die chinesische Botschaft in Berlin bereits angedeutet hat.

Huawei auf Angriffe vorbereitet

Eine eindeutige Positionierung in der Huawei-Frage fällt deswegen schwer, weil bislang zwar starke Vermutungen bezüglich möglicher Abhöraktionen im Raum stehen, eindeutige Belege dafür jedoch fehlen. Huawei seinerseits bestreitet naturgemäß sämtliche Vorwürfe, geht aber gleichzeitig davon aus, dass sich der Streit, befeuert durch weitere Eskalationen mit US-Präsident Donald Trump, auch 2020 fortsetzen wird.

Auf dem Weltwirtschaftsforum in Davos ließ Huawei-Chef Ren Zhengfei verlauten, dass man sich mittlerweile besser auf die „Angriffe“ vorbereitet sehe. Einerseits spielte Ren Zhengfei wirtschaftliche Auswirkungen herunter, gleichzeitig sagte er, man habe im vergangenen Jahr einiges an Erfahrungen gesammelt, nun ein stärkeres Team zusammengestellt und sei optimistisch, dass man im Konzern auch mit weiteren Vorwurfswellen gut zurechtkommen werde.

Die US-Regierung hatte US-Firmen die Zusammenarbeit mit Huawei im vergangenen Jahr tatsächlich verboten. Die Behörden begründeten den Schritt mit der „nationalen Sicherheit“. Weiters übt man seitens der USA auch Druck auf Staaten in der EU aus.

Wie die Spionage funktionieren könnte

Aber wie würde das Szenario eigentlich aussehen, sollten die Befürchtungen zutreffen und Huawei tatsächlich einen Lauschangriff auf andere Nationen starten? Rene Mayrhofer und Andreas Springer, beide ebenfalls Professoren an der Johannes Kepler Universität Linz, erläutern die technischen Vorgänge: „Die Daten kommen über die Basisstationen (Funkmasten) vom Mobiltelefon bzw. zum Mobiltelefon. In der Basisstation, oder auch in anderen Knoten im Netzwerk, könnte dann – unbemerkt von der Benutzerin oder dem Benutzer – mitgehört werden“, sagt Andreas Springer. Damit könne nicht nur spioniert werden, wer welche Daten überträgt, sondern auch, wer sich wann wo aufhält und wer wie lange mit wem kommuniziert bzw. auf welche Daten oder Dienste zugreift. „Allerdings ist anzumerken, dass so eine extrem große Datenmenge zu verarbeiten und auch zum sogenannten „Spion“ weiter zu übertragen wäre, was technisch eine große Herausforderung darstellt“, so Springer. „Aber auch aufgrund der notwendigen Datenübertragung, etwa zu einem Rechenzentrum des „Spions“, wäre das nicht so einfach zu verschleiern.“

Man müsse außerdem unterscheiden zwischen Geräten im sogenannten Backend, also in der Infrastruktur für Netzbetreiber (wie zum Beispiel im Mobilfunknetzwerk) und Endgeräten wie Smartphones. „Die möglichen Szenarien sind sehr unterschiedlich“, ergänzt Rene Mayrhofer, der an der JKU das Institut für Netzwerke und Sicherheit leitet.

Bei Backend-Geräten könnten Datenströme, die über diese Geräte laufen, abgehört oder manipuliert werden, so Mayrhofer. „Dazu müssten solche Geräte aber direkten Kontakt mit Servern der möglicherweise abhörenden Organisationen haben oder diese Organisationen den Datentransfer generell abgreifen können.“ Ein Abhören könne dann entweder durch Fehler in der Software – die dem Hersteller nicht bekannt sind, aber von Angreifern gefunden wurden – ermöglicht werden. „Oder durch bewusst eingebaute Hintertüren. Jedes komplexe System hat Fehler, und ich halte die Gefahr schlechter Produkte für deutlich größer als die, dass Hintertüren bewusst eingebaut werden“, sagt der Experte.

„Netzbetreiber sollten ohnehin Netzwerkarchitekturen präferieren, die sich nicht auf die vollständige Sicherheit einzelner Komponenten verlassen“, meint Mayrhofer. Das

bedeutet laut dem Experten konkret, dass sich Backend-Geräte nicht unkontrolliert direkt mit Servern anderer Organisationen verbinden dürfen, sondern nur durch entsprechend kontrollierte Kanäle. „Kommunikation über Hintertüren sollte damit zumindest nach gewisser Zeit auffallen“, so Mayrhofer.

Wenn Hersteller zu viele unbeabsichtigte Fehler in den eigenen Produkten haben, die nicht zeitnah durch Updates geschlossen werden, seien jedenfalls alle Kundinnen und Kunden dieser Produkte betroffen und möglichen Angriffen ausgesetzt, erklärt der Experte. Das treffe auf beides – Backend und Endgeräte – zu. „Die Frage nach dem Ablauf möglicher Spionageaktivitäten ist daher eine der Produktqualität: Gute Produkte und gute Netzwerkarchitekturen erschweren es, schlechte Produkte bieten viel Potenzial“, sagt Mayrhofer. „Sichere Hintertüren, die nur der Hersteller oder ein Land nützen kann, andere aber nicht finden werden, sind mir keine bekannt“, betont der Experte. „Wenn jemand in der Lage ist, solch perfekte Hintertüren zu bauen, sollte auch der Rest des komplexen Systems komplett fehlerfrei sein – und das habe ich in Jahrzehnten noch nicht in der Praxis gesehen.“

Eine Frage des Preises

Noch ist schwer abzuschätzen, ob man sich in den EU-Ländern darauf einlassen wird, Huawei den Netzausbau zu überlassen, oder sich doch lieber auf europäische Alternativen wie Ericsson oder Nokia festlegt. Das grundlegende Problem beim 5G-Aufbau ist wohl auch, dass es nicht besonders viele Anbieter gibt, schon gar nicht, die bei der Technologie mit Huawei mithalten können. Das chinesische Unternehmen besticht vor allem auch mit seinen Preisen, die – wie man in der Branche vernimmt – gegenüber der Konkurrenz wohl niedrig sind.

„Ich nehme an, dass man Komponenten von Huawei sehr wohl einsetzen wird“, so die Einschätzung Mayrhofers. „Allerdings sollten alle Produkte solcher Komplexität immer überwacht werden, und man sollte sich nicht auf ein einzelnes Gerät für die Sicherheit des gesamten Systems verlassen.“ Vielleicht könne es künftig auch sinnvoll sein, Backend-Geräte von Huawei im eigenen Netzwerk besonders isoliert zu betreiben, um Erfahrungen mit dem Betrieb und Verhalten zu sammeln, so der Experte. „Vertrauen wird immer nur langsam aufgebaut und kann bei erkanntem Fehlverhalten auch schnell verloren sein. Wenn man vorsichtig vorgeht, sollte kein Grund zu Panik-Entscheidungen bestehen.“

NEWS 13.03.2020

Wissen

Erschienen in [Ausgabe 1/2020](#)

Was bringt 5G?

5G ist die nächste bzw. 5. Mobilfunkgeneration, die die aktuell im Einsatz befindliche LTE-Technik ablösen soll. Versprochen werden mehr Bandbreite und kürzere Latenzzeiten – also weniger Verzögerung zwischen Sender und Empfänger. LTE (oder auch 4G) schafft derzeit eine Datenrate von maximal 300 Megabit pro Sekunde und eine Latenzzeit von unter zehn Millisekunden. 5G jedoch soll es künftig

auf eine Datenrate von bis zu 20 Gigabit pro Sekunde und weniger als eine Millisekunde Latenzzeit bringen.

Die Einsatzszenarien sind vielfältig, und 5G fällt als Begriff oft in Zusammenhang mit einem anderen Schlagwort: Internet der Dinge. Egal, ob man von vernetztem oder autonomem Fahren spricht, von Sensoren generell, die in Echtzeit miteinander kommunizieren, von Multiplayer Games am Handy, Filmen in 4K-Auflösung oder Drohnen, die via Mobilfunk gesteuert werden – 5G ist derzeit in aller Munde.

Laut Schätzungen des Informationsdienstleisters IHS soll es bis zum Jahr 2030 30 Milliarden vernetzte Dinge geben. Ganz besonders interessant könnte es auch für Unternehmen werden, gleich ganze Teile des Mobilfunknetzes für sichere, interne Kommunikation zu reservieren. Auch für die Industrie, wenn es etwa um ferngesteuerte Roboter geht, wird 5G ein Thema sein. Generell wird das neue, schnellere Netz zunächst einmal vor allem im Businessbereich eine Rolle spielen. Denn beim Privatgebrauch von WhatsApp, Smartphone Games und Social Media wird man erst einmal keine großen Unterschiede bemerken.

Für Debatten sorgt 5G auch immer wieder in Sachen Gesundheit. Viele fürchten sich vor schädlichen Strahlen. Bisher gibt es jedoch keine konkreten Hinweise darauf, dass 5G oder Mobilfunktechnologien generell krebserregende Effekte haben könnten. Hinzu kommt, dass die Strahlengrenzwerte für den 5G-Standard gemeinsam mit der Weltgesundheitsorganisation (WHO) und weiteren Expertinnen und Experten erarbeitet und festgelegt wurden.

[Zurück zur Übersicht](#)

JOHANNES KEPLER UNIVERSITÄT
Altenberger Straße 69
4040 Linz, Österreich

T: +43 732 2468 0
F: +43 732 2468 4929
info@jku.at