LBBW Bereit für Neues

Corporates Blickpunkt

LBBW Research | Corporates

Telekommunikation - Aufbau der 5G Netze

»Warum es keine 100%ige Sicherheit geben wird

Uwe Burkert

Chefvolkswirt und Leiter Research

LBBWResearch@LBBW.de

LBBW_Research

Executive Summary

- **Die neue Technologie 5G wirft Fragen zur Sicherheit des Equipments und der digitalen Netze auf. Wie sicher können digitale Netze überhaupt sein?**
- **5G aus Sicherheitsaspekten betrachtet ist Bestandteil einer für Deutschland kritischen Infrastruktur. Dem gegenüber stehen auf Seiten der Technologie systemimmanente Fehlerquellen in Hard- und Software.**
- **Warum wir bei 5G-Equipment aus China vorsichtig sein sollten.**

Inhalt

Autoren:

Bettina Deuscher

Senior Investment Analyst

+49 (0) 711/ 127 – 73 10 5

bettina.deuscher@LBBW.de

Mirko Maier

Senior Investment Analyst

+49 (0) 711/ 127 - 73 26 4

mirko.maier@LBBW.de

ERSTELLT AM: 14.10.2019 14:10 ERSTMALIGE WEITERGABE AM: 14.10.2019 14:12

01 I Sicherheit der Netze

Warum es keine 100% sicheren Netze geben wird

Industrie 4.0 bedeutet Digitalisierung der industriellen Geschäftsmodelle. Digitalisierung geht einher mit Vernetzung von Geräten bzw. Dingen, von ganzen Wertschöpfungsketten und im Internet der Dinge (IoT) auch bis zum Endkunden. Die Vernetzungen dieser digitalen Plattformökonomien erfolgen mithilfe von kabelgebundenen oder mobilen Netzen.

Nur ein in sich geschlossenes, autarkes, von der Außenwelt völlig abgeschottetes IT-System oder Kommunikationsnetz kann als nahezu sicher gelten. Dies ist der Grund, warum Atomkraftwerke keinen Internetanschluss haben (sollen). Vor diesem Hintergrund wagen wir die These, dass es in der digitalen Welt von morgen, in der beginnenden Ära des Internets der Dinge, nie zu 100% sichere Netze geben wird. Es genügt, einen Rechner, eine Maschine, einen Sensor ans Internet anzubinden und die systemimmanenten Einfallstore der Informations- und Kommunikationstechnologie stehen offen.

Nur geschlossene Systeme sind sicher

Systemimmanent deswegen, weil ITK (Informations-, Technologie- und Kommunikations) -Equipment aus Hard- und Software besteht. Hardware, die arbeitsteilig in weltweit verteilten Wertschöpfungsketten hergestellt wird, dementsprechend auch dem Zugriff Unberechtigter ausgesetzt sein kann. 2015 wurden laut einem Bericht des US-Magazins Bloomberg Businessweek von Apple und Amazon Spionagechips auf vom US-Unternehmen Super Micro in Asien hergestellten Motherboards entdeckt. Apple verwendete die Boards in den Servern seiner Datenzentren und Amazon in seinen Serverfarmen von Amazon Web Services (AWS), dem weltweit erfolgreichsten Cloud-Computing-Service. Die Chips sollen am Baseboard Management Controller angedockt gewesen sein, der die Schnittstelle zwischen Systemsoft- und Hardware verwaltet. Ein Zugang von Extern auf die Server wäre damit möglich gewesen, so Bloomberg. Der US-Geheimdienst konnte die Spur der Chips anscheinend bis China verfolgen.

Angriffspunkte: Hardware und …

Ohne Software läuft kein noch so kleines Tech-Gadget. Software hat mehrere kritische Dimensionen. Erstens wird Software (immer noch) von Menschen gemacht. Zweitens ist Software einem zügigen Alterungsprozess unterworfen und drittens kann Software nicht Esperanto.

Das Internet der Dinge besteht aus vielen Komponenten, vom kleinsten Sensor über die Mobilfunkbasisstation bis hin zur Serverfarm. Die Verbindungen erfolgen über unzählige Gateways, über die sich Cyberkriminelle Zugang zu Netzwerk- und Infrastruktursystemen verschaffen können. Gemeinsam ist ihnen, dass ihr Softwarecode von Menschen erstellt wurde. Das allein ist eine stete Fehlerquelle, die sich schon die ersten Hacker des MIT (Massachusetts Institute of Technology, Cambridge, USA) in den 50er-Jahren zunutze machten. Programmierfehler passieren unbeabsichtigt, werden irgendwann entdeckt und idealerweise vom Hersteller in Form von Update's gepatcht. Ein Prozess, der jedem Windows-

… Software

user geläufig ist. Manche dieser unbeabsichtigten Programmierfehler erlauben den Zugriff Dritter. Wird diese Lücke bzw. Backdoor von den „Guten“ entdeckt, melden sie diese dem Hersteller damit er sie patchen und damit schließen kann. Finden die „Bösen“ die Lücke zuerst, wird sie entweder sofort für eine Attacke genutzt, für spätere Aktionen aufgehoben oder im sogenannten Darknet meistbietend verkauft.

Backdoor: Fahrlässig entstanden oder vorsätzlich geschaffen?

Von den fahrlässig geschaffenen Backdoors unterscheiden sich die vorsätzlich in die Software heimlich integrierten Hintertüren. Je stärker die Verbreitung bzw. je höher der weltweite Marktanteil einer wesentlichen Kernkomponente (z.B. Betriebssystem, Applikation, Router, Switches, etc.) eines ITK-Netzes, umso interessanter wird diese für Dritte um darüber unerlaubt Kommunikation mitzuhören und Daten abzusaugen. Implantierte Backdoors sind schwer nachzuweisen. Sie werden im Zusammenhang mit Geheimdienstaktivitäten öfters genannt.

Software altert schnell. Smartphonenutzer kennen den frustrierenden Moment, wenn die gewünschte neue App aus Apple‘s App Store oder von Google Play den Download verweigert, weil das Betriebssystem des Smartphones veraltet sei. Ein dezenter Hinweis, dieses doch bitte upzudaten oder, falls vom Smartphonehersteller kein Update zur Verfügung steht, eine Neuanschaffung zu überlegen. Laut der russischen Virensoftware Kaspersky laufen 10% der PC’s mit einem nicht mehr mit Updates versorgten Betriebssystem wie z.B. Windows XP. Weiteren 31% an Windows 7-Nutzern droht Anfang 2020 das Supportende. Keine Updates bedeuten nicht nur keine Apps, sondern auch keinen Schutz mehr vor den neuen Bedrohungen aus den auf Hochtouren laufenden Innovationslaboren der Hacker.

Mit „Software kann kein Esperanto“ meinen wir die Probleme, die sich aus der mangelnden Interoperabilität der Komponenten einer ITK-Infrastruktur untereinander ergeben können. Da die verschiedenen Komponenten im Internet der Dinge miteinander kommunizieren müssen, ergeben sich aus deren Interaktion zusätzliche Fehlerquellen. Ein Softwareupdate einer einzigen Komponente eines bislang stabilen Systems kann zu unerwarteten Problemen führen. So wie eines der jüngsten Windowsupdates in bestimmten NEC-Notebooks die Kommunikation zwischen den verbauten Intel Chips und den von Broadcom stammenden WLAN-Karten verhinderte. Die zunehmende Komplexität der digitalen Infrastrukturen verstärkt diese Interoperabilitätsprobleme immer mehr. Die Vorstellung, der Mensch sei das schwächste Glied einer stabilen IT-Sicherheitskette, erscheint mittlerweile als überholt. Laut Enisa (European Union Agency for Network and Information Security) entfielen 67% der Ausfälle in den europäischen Kommunikationsnetzen auf Systemfehler, die mehrheitlich auf Probleme mit der Software zurückzuführen sind. Der Faktor Mensch steht mit klassischen Bedienungsfehlern wie z.B. durchtrennte Kabel, etc. für lediglich 18% der Ausfälle.

Viele verschiedene Komponenten sollen fehlerfrei 24/7 interagieren

Kritische vs. unkritische Infrastrukturen

Werden die Passwörter von Online-Shoppern gehackt, ist das für den einzelnen mehr als ärgerlich, vielleicht gar mit einem finanziellen Verlust verbunden. Auch für das gehackte Unternehmen wiegt der Reputationsschaden schwer. Aber in ihrer Existenz dürften deswegen weder die wenigsten Konsumenten noch Unternehmen gefährdet sein. Anders sieht

dies aus, wenn über Kommunikationsnetze verschickte geheime Konstruktionsdaten auf ihrem Weg bspw. vom Hersteller zum Zulieferer abgegriffen werden. Ein Worstcase aus sicherheitspolitischer Sicht wäre der großflächige Kontrollverlust über nationale Infrastrukturen wie Strom-, Wasser und Kommunikationsnetze.

Einer im März 2019 durchgeführten Umfrage des Ponemon Institutes zufolge haben 90 Prozent der Unternehmen, die auf industrielle Informationstechnologie z.B. in der Fertigung, Pharmabranche und im Transportwesen setzen, in den letzten zwei Jahren zumindest einen großen Cyberangriff erlebt. 50% der befragten Unternehmen wurden in den letzten zwei Jahren Opfer eines Angriffs auf betriebsnotwendige Infrastruktur und mussten Ausfälle hinnehmen. Produktionsausfälle können negative Auswirkungen etwa in der Just-in-Time-Produktion und damit in der Wertschöpfungskette bis hin zum Kunden nach sich ziehen, was i.d.R. finanzielle Verluste bedeutet. Auch sind Angriffe auf Stromversorgungen schon vorgekommen und das Kapern von Autos via Remote Hacks in deren Bordcomputer sind nicht nur theoretisch möglich. Wenig tröstlich, dass Terroranschläge mit Hilfe des Internets laut Expertenaussagen wohl erst in einigen Jahren drohen.

Knipsen bald Hacker in Deutschland das Licht aus?

Dementsprechend sind die aktuellen Diskussionen um Sicherheitsstandards beim Aufbau von 5G-Netzen nachvollziehbar. Via 5G wird in der Zukunft der Großteil der vom Internet der Dinge, der Industrie 4.0-Anwendungen und den künftigen Smart Cities produzierten Daten per Funk übertragen. 5G ist daher u.E. durchaus aus Sicherheitsaspekten als Bestandteil einer für Deutschland kritischen Infrastruktur zu bezeichnen.

BSI: Deutschlands Technologie-TÜV

In Deutschland soll uns das Bundesamt für Datenschutz (BSI) vor „Computerversagen, -missbrauch oder -sabotage“ schützen. Hierzu zählt auch die Überprüfung kritischer Infrastrukturkomponenten für in Deutschland verbauter Netzwerkkomponenten für 5G. Letztendlich u.E. ein vergleichbarer Wettlauf wie der von realen Verbrechern und der Polizei, im Zweifel ist auch im Virtuellen der Hacker immer einen Schritt voraus.

Mehr Sicherheit im Netz nur mit 100% 5G-Equipment

5G ist sicherer, aber nicht sicher

In den technischen Spezifikationen von 5G wurden gegenüber dem Vorgänger 4G bzw. LTE verschiedene Sicherheitsparameter eingeführt bzw. verbessert. Dies soll u.a. dazu dienen, insgesamt sicherere Netze aufzubauen. Hervorzuheben sind neue kryptografische Lösungen, die die 5G Komponenten getrennt voneinander absichern sollen. Wurde eine Komponente gehackt, besteht so weiterhin der Schutz der anderen Netzkomponenten. Des Weiteren soll mit der Technik „Authentication Confirmation" (AC) für mehr Sicherheit beim Roaming gesorgt werden. Hier schickt das Endgerät des Teilnehmers einen kryptografischen Beweis über die Identität des Mobilfunkanbieters, in dessen Netzwerk sich das Endgerät eingewählt hat, zurück an den Mobilfunkbetreiber des Smartphone-Users. Nennenswert erscheint uns auch die künftige Verschlüsselung der Langzeitidentität der Teilnehmer (IMSI). Diese dient insbesondere dem Schutz sensibler Nutzerdaten.

Gegenüber 2G/3G/4G-Netzen bedeuten diese Features eine Weiterentwicklung sicherheitsrelevanter Parameter. Doch nur in einem „reinen" 5G-Netz wirken sich die Sicherheitsvorteile voll aus. Das BSI thematisiert diesbezüglich u.E. zu Recht die Migrationsgeschwindigkeit der bestehenden Netze auf 5G. Doch die Migration ist weder vom Prozess (z.B. welche Netzkomponenten zuerst) noch von der Geschwindigkeit (z.B. binnen X Jahren) in den 5G-Spezifikationen definiert. Der Gesetzgeber hat sich diesbezüglich auch in den Bedingungen der bislang erfolgten Frequenzversteigerungen nicht geäußert, wohl auch aus Rücksicht auf die noch per 4G zu schließenden Funklöcher. Von Seiten der Nachfrage wird sich u.E. der Migrationsdruck auch in Grenzen halten. Viele Anwendungen für Endkonsumenten brauchen gar kein 5G. Manche der 5G-Vorteile, wie z.B. die schnelleren Übertragungsraten, können durchaus mit bestehenden LTE-Netzen erzielt werden, was den Migrationsdruck zusätzlich mindert. Was ist das Fazit? U.E. wird es noch sehr lange dauern, bis die neuen Sicherheitsmechanismen von 5G zum Tragen kommen.

Huawei – Ein Risiko für unsere Sicherheit?

China's technologische Aufholjagd

Die Chinesen haben seit 2015 einen klar kommunizierten Plan. 100 Jahre nach der 1949 erfolgten Staatsgründung wollen sie die führende Industrienation der Welt sein. Die auf dem Weg dahin definierten Zwischenziele, wie z.B. Made in China 2025, bedingen im Rahmen von landesweiten Initiativen bedeutende Fortschritte u.a. in der Informations- und Kommunikationstechnologie. Eine technologische Aufholjagd ohnegleichen. Ein Sprung von der verlängerten Werkbank des Westens zum technologisch führenden Land in wenigen Jahren. Ein Akt, der nur aus eigener Kraft kaum zu schaffen wäre. Viel an externem Know-how wird hierfür benötigt. Dementsprechend sind die chinesischen Auslandsinvestitionen in die Höhe geschossen. Allein in Deutschland wurden 2016, dem bisherigen Peak, 68 Unternehmen aufgekauft. Seit 2005, lt. einer aktuellen Analyse von Ernst & Young, addiert über 350. Erst seit Kuka hat sich die öffentliche, und damit auch die politische, Wahrnehmung zu diesem in großem Stil ablaufenden Technologietransfer allmählich gewandelt. Der Bundesverband der Deutschen Industrie (BDI) schlägt inzwischen gar Alarm: "Trotz der starken Anziehungskraft des chinesischen Marktes wird es für

Unternehmen immer wichtiger, mögliche Risiken eines Engagements in China im Auge zu behalten." Damit ist nicht nur die schärfere Rivalität mit technologisch zunehmend auf Augenhöhe agierenden chinesischen Konkurrenten gemeint, sondern auch die Furcht vor Industriespionage. Sieben von zehn deutschen Industrieunternehmen sind nach Angaben des Digitalverbands Bitkom 2016 und 2017 Opfer von solchen illegalen Aktivitäten geworden, darunter auch Sabotage und Datendiebstahl. Fast jedes fünfte betroffene Unternehmen nannte China als Ausgangsort.

Die aktuelle Diskussion um die Sicherheit chinesischer Equipmentlieferanten ist nicht neu. Seit 2005 wird dies mit unterschiedlicher Intensität in Ländern wie Australien, England, Neuseeland und USA thematisiert. Die kolportierte Nähe des chinesischen Anbieters zum Staat lässt Ängste aufkeimen, die von Industriespionage bis Cyberkrieg reichen. Huawei erwehrt sich dieses Verdachts. Das Unternehmen bestreitet u.a. Backdoors in seine Produkte für Spionagezwecke einzubauen. Vorsätzliche Backdoors sind u.E. auch nicht das wirkliche Problem. Kritisch sind u.E. die durch Fehler in der Programmierung fahrlässig geschaffenen Backdoors. Anfang 2019 wurde publik, dass bei unter dem Namen MateBook (das vergleichbare Apple-Produkt heißt MacBook) von Huawei hergestellten Business-Notebooks ein gravierender Softwarefehler entdeckt wurde. Der Bug hätte bzw. hat Dritten die Übernahme der Kontrolle über das Notebook erlaubt. Zum Zeitraum in dem der Zugriff möglich war, gab es keine Aussage. Huawei hat nach Hinweisen aus den USA den Fehler gefixt. Dieses Beispiel zeigt u.E., dass die Aussage, aktiv keine Backdoors einzubauen, nicht vor fahrlässig entstandenen Hintertüren schützt.

Huawei – eine konfuzianische Erfolgsgeschichte?*

- Gegründet - 1997 von Ren Zhengfei, Ex-General der chinesischen Volksarmee
- Einstieg in Netzwerktechnologie - 2003 von Cisco, USA, wegen Diebstahl geistigen Eigentums verklagt. Huawei soll Teile des Betriebssystems für Router, Switches, Handbücher, etc. kopiert haben.
- Einstieg in Mobilfunktechnologie - Ab 2000 soll Huawei über mehrere Jahre mit gestohlenen Passwörtern von Nortel, Kanada, technische Dokumentationen, Entwicklungsprojekte und Geschäftspläne gestohlen haben.
- Einstieg in die Handyproduktion - 2008 wurden von Motorola, USA, fünf ehemalige, chinesischstämmige Mitarbeiter wegen Diebstahl geistigen Eigentums im Auftrag von Huawei verklagt. 2010 wurde die Klage auf Huawei ausgeweitet.

*Konfuzius: "Wer große Meister kopiert, erweist ihnen Ehre."

Quelle: LBBW Research

Wir müssen zugestehen, dass sich unser Vertrauensvorschuss in die Sicherheit kritischer Netzkomponenten von Huawei in Grenzen hält. In den Weiten des Internets lassen sich genug Pressemeldungen, Firmenstatements, Aussagen ehemaliger CEO's von Unternehmen, etc. finden, die Huawei in Zusammenhang mit Industriespionage bringen.

Verurteilungen im Sinne von ergangenen Gerichtsurteilen zu Lasten des Unternehmens Huawei gab es u.W. keine. Der Marktzugang zu China war zumindest in der Vergangenheit stets ein gewichtiges Argument, das auch die immer wieder aufkeimenden europäischen Dumpingvorwürfe gegen die chinesischen Anbieter Huawei & Co. zuverlässig zum Schweigen brachte. Details der u.W. mehrheitlich außergerichtlich geschlossenen Einigungen sind uns nicht bekannt, deren bloße Existenz reicht aber u.E. für eine gewisse Skepsis gegenüber Huawei.

„Vertrauen der Kundschaft und der Ruf der Ware ist mehr wert, als ein vorübergehender Nutzen.“ Robert Bosch

Entweder…oder

Die Bedenken um die Beteiligung von Huawei an Deutschlands 5G-Ausbau artikulieren sich im Vertrauen in die Kompetenzen des BSI bis hin zum Verbot. Länder wie z.B. Australien und Neuseeland folgen der Vorgehensweise der USA und schließen chinesische Anbieter bei ihren lokalen Auftragsvergaben für 5G-Netze von vornherein aus. Auch in Deutschland mehren sich die Stimmen, die wie der Parteichef der Grünen Robert Habeck den Ausschluss Huawei‘s fordern. In England versucht sich der britische Telekommunikationskonzern BT u.E. durchzumogeln und entfernt Equipment von Huawei nur aus seinen auf 5G zu migrierenden 3G und 4G-Kernnetzen bzw. dem landesweiten Backbone. Durchmogeln deshalb, da bei speziellen 5G-Anwendungen wie z.B. dem autonomen Fahren solch hohe Datenmengen anfallen, die enorme Rechenpower schon im dem Backbone vorgelagerten Radio Access Network (RAN) und damit bei den Mobilfunkbasisstationen erforderlich machen. Nutzt BT Huawei-Equipment weiterhin in diesem sogenannten EDGE-Computing genannten Anwendungsszenario, läuft der gewünschte Spionageschutz u.E. ins Leere.

Fazit

5G-Netze sind u.E. aus Sicherheitsaspekten als Bestandteil einer für Deutschland kritischen Infrastruktur zu betrachten. Dass das BSI kritische Infrastrukturkomponenten für in Deutschland verbaute Netzwerkkomponenten prüft, ist dementsprechend richtig und wichtig. Einen 100%igen Schutz vor Cyberkriminalität wird es dennoch nicht geben. Vor dem Hintergrund der voranschreitenden Digitalisierung unserer Industrie und unseres Lebensumfeldes sollte das Augenmerk darauf liegen, die möglichen Gefahrenquellen so klein wie möglich zu halten. Hierzu gehört u.E. auch eine vorsichtige Vorgehensweise bei der Auswahl der Lieferanten von 5G-Equipment. In Bezug auf Huawei müssen wir leider konstatieren, dass deren Leumund u.E. nicht der Beste ist. Ein Aufbau von 5G-Netzen in Deutschland bzw. Europa ohne chinesische Anbieter wäre u.E. möglich. Er wird vielleicht teurer, weil die europäischen Player mangels staatlicher Unterstützung nicht die günstigen Absatzfinanzierungen ihrer chinesischen Wettbewerber darstellen können. Technologisch betrachtet wären aber die von den europäischen Anbietern gebauten 5G-Netze denen ihrer chinesischen Konkurrenz ebenbürtig.

Vorsicht bei der Auswahl der 5G-Lieferanten ist geboten

Disclaimer:

Bitte beachten Sie:

Diese Publikation richtet sich ausschließlich an Empfänger in der EU, Schweiz und Liechtenstein.
Diese Publikation wird von der LBBW nicht an Personen in den USA vertrieben und die LBBW beabsichtigt nicht, Personen in den USA anzusprechen.

Aufsichtsbehörden der LBBW: Europäische Zentralbank (EZB), Sonnemannstraße 22, 60314 Frankfurt am Main und Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), Graurheindorfer Str. 108, 53117 Bonn / Marie-Curie-Str. 24-28, 60439 Frankfurt.

Diese Publikation beruht auf von uns nicht überprüfbaren, allgemein zugänglichen Quellen, die wir für zuverlässig halten, für deren Richtigkeit und Vollständigkeit wir jedoch keine Gewähr übernehmen können. Sie gibt unsere unverbindliche Auffassung über den Markt und die Produkte zum Zeitpunkt des Redaktionsschlusses wieder, ungeachtet etwaiger Eigenbestände in diesen Produkten. Diese Publikation ersetzt nicht die persönliche Beratung. Sie dient nur zu Informationszwecken und gilt nicht als Angebot oder Aufforderung zum Kauf oder Verkauf. Für weitere zeitnähere Informationen über konkrete Anlagemöglichkeiten und zum Zwecke einer individuellen Anlageberatung wenden Sie sich bitte an Ihren Anlageberater..

Wir behalten uns vor, unsere hier geäußerte Meinung jederzeit und ohne Vorankündigung zu ändern. Wir behalten uns des Weiteren vor, ohne weitere Vorankündigung Aktualisierungen dieser Information nicht vorzunehmen oder völlig einzustellen.

Die in dieser Ausarbeitung abgebildeten oder beschriebenen früheren Wertentwicklungen, Simulationen oder Prognosen stellen keinen verlässlichen Indikator für die künftige Wertentwicklung dar.

Die Entgegennahme von Research Dienstleistungen durch ein Wertpapierdienstleistungsunternehmen kann aufsichtsrechtlich als Zuwendung qualifiziert werden. In diesen Fällen geht die LBBW davon aus, dass die Zuwendung dazu bestimmt ist, die Qualität der jeweiligen Dienstleistung für den Kunden des Zuwendungsempfängers zu verbessern.