Whitepaper zur Diskussion über die Sicherheit der Huawei-Netzwerktechnik:

1. Vorwort: der Stand der Dinge

Während die Versteigerung der 5G-Infrastrukturen noch im Gange ist/ihrem Ende entgegengeht, hat sich die Bundesregierung im Einklang mit der EU-Kommission mittlerweile festgelegt: die Bundesrepublik wird Huawei nicht vom Aufbau der 5G-Infrastruktur ausschließen. Vorausgegangen waren monatelange Diskussionen darüber, ob die kritische Telekommunikationsinfrastruktur mit Netzgeräten aus China und insbesondere von Huawei betrieben werden darf. Besonders augenfällig wurde diese Diskussion, als der US-Botschafter Richard Grenell noch am selben Tag, als die Bundesnetzagentur neue Sicherheitsbestimmungen für Netzbetreiber vorgeschlagen hatte, die Haltung der Vereinigten Staaten dazu erklärte. Er drohte in einem Brief an Wirtschaftsminister Peter Altmaier mit einer empfindlichen Einschränkung der Geheimdienstzusammenarbeit, wenn Deutschland weiter auf Huawei setzte.

Hintergrund sind zwei Problemfelder, die in Zusammenhang mit Huawei bestehen sollen: Zum einen sei dies Angst vor Spionage, die der Netzbetreiber aufgrund von chinesischen Gesetzen und im Auftrag chinesischer Nachrichtendienste durchführen würde und so sensible Daten chinesischen Behörden zur Verfügung stellen könnte. Zweitens bestehen Bedenken, dass Huawei in einer internationalen Krise von der chinesischen Regierung dazu veranlasst werden könnte, ausländische Netze zu stören oder gar lahmzulegen. Sabotage lautet das Stichwort. Ein sogenannter „Kill-Switch“ würde von einem Moment auf den nächsten die gesamte Infrastruktur lahmlegen, so die These.

Um solcherlei Funktionen zu entdecken, bedarf es des Einblicks in die Quellcodes des Anbieters. Großbritannien verpflichtete Huawei dazu und bemängelte im Zuge der Überprüfung nachlässige Ingenieurarbeit und etwaige Sicherheitslücken in der Lieferkette. Indes glauben die Sicherheitsexperten von der Insel nicht, dass die gefundenen Probleme durch staatliche Einflussnahme entstanden seien. Folgerichtig will die britische Regierung den chinesischen TK-Ausrüster nicht vom Aufbau des 5G-Mobilfunknetzes im Königreich ausschließen. Geliefert werden dürften aber nur Teile, bei denen die Gefahr von Spionage oder Sabotage gering sei. Dazu gehören z. B. Basisstationen, Antennen und bestimmte Übertragungstechnik. Die wichtigsten und sensibelsten Bereiche der Netzinfrastruktur sollen aber ohne das Equipment aus China laufen. Ein Restmisstrauen ist also weiterhin vorhanden.

Die Bundesregierung und die zuständigen Behörden wie die Bundesnetzagentur und das BSI, aber auch die Gesellschaft für Informatik (GI) schätzen die Situation etwas anders ein als Großbritannien. So hat Berlin im März die Sicherheitsanforderungen erhöht, aber für alle Anbieter. Ein neuer Katalog mit Sicherheitsfragen muss künftig eingehalten werden. Im Kern handelt es sich um eine Art Beweislastumkehr. Netzbetreiber müssen belegen, dass jegliche in Kritischen Infrastrukturen eingesetzte Telekommunikations-Technik vertrauenswürdig ist.

Der Präsident der Bundesnetzagentur Jochen Homann erklärte in einem Interview mit der Financial Times: „Die Bundesnetzagentur hat keine konkreten Anhaltspunkte gegen Huawei erhalten. Wir kennen auch keine andere Einrichtung in Deutschland, die verlässliche Hinweise erhalten hat."[1] Arne Schönbohm, Präsident des BSI hat

[1] https://www.ft.com/content/a7f5eba4-5d02-11e9-9dde-7aedca0a081a

bereits im November 2018 erklärt, dass seiner Behörde keine Belege für potenzielle Risiken durch Huawei-Produkte vorlägen. Ganz im Gegenteil wünschte sich Schönbohm bei der Eröffnung eines Huawei-Sicherheitslabors in Bonn ähnliche Aktivitäten von anderen Herstellern. In dem Labor können Kunden u. a. den Quellcode von Huawei-Produkten prüfen. Schönbohm hatte bei der Gelegenheit auch unterstrichen, dass sich seine Security-Spezialisten Huawei-Bauteile weltweit beschafften, um sie zu untersuchen – unabhängig vom konzerneigenen Labor.

Der TK-Ausrüster und Handy-Hersteller hat die Vorwürfe wiederholt zurückgewiesen. So erklärte im Interview mit der Welt Richard Yu, Leiter der Consumer Business Group, zu der das Smartphone-Geschäft gehört: „Das ist Unsinn, weil es technisch nicht möglich ist. Und wir würden es auch gar nicht zulassen. Wir haben in unserer Hard- und Software sehr hohe Sicherheitsstandards.“[2]

In einem umfangreichen Whitepaper zur Thematik hat Huawei die Bedeutung von Cybersecurity und Datenschutz verdeutlicht: „In der digitalen Welt der Einsen und Nullen ist Sicherheit eine notwendige Voraussetzung, durch die erst alles andere möglich wird. Cybersecurity und Datenschutz haben bei Huawei höchste Priorität. Sie sind Teil unserer DNA, kodiert in allen unseren Abläufen, Audits, Prozessen, Richtlinien, Produkten und Dienstleistungen. Wir haben ein globales Sicherungssystem für Cybersicherheit aufgebaut und implementiert, das jeden Prozess von Ende zu Ende abdeckt.“

Ähnlich äußert sich die Gesellschaft für Informatik, die die Vorwürfe gegen Huawei ideologisch begründet sieht und eine Auswahl der 5G-Netzausrüster streng nach technischen und wirtschaftlichen Parametern fordert. Die gegen Huawei geäußerten Vorwürfe würde man auch Cisco, Nokia und Ericsson machen können.

Der Sprecher des GI-Präsidiumsarbeitskreises, Prof. Hartmut Pohl, kommentierte: „Auch wenn ein IT-System bereits geprüft wurde und Sicherheitslücken erkannt wurden, können in Zukunft immer weitere offenbar werden. Grundsätzlich kann nicht nachgewiesen werden, dass ein IT-System frei von Sicherheitslücken und damit auch von Angriffspunkten ist. Dasselbe gilt für von Herstellern bewusst in IT-Systeme eingebaute Hintertüren, die einen unautorisierten Zugriff ermöglichen."[3]

Demnach besteht also ein gewisses Restrisiko, eine Restsicherheitsgefahr. Was wäre, wenn ein Netzgerätehersteller, Cisco oder Huawei zum Beispiel, doch Daten aus Kritischen Infrastrukturen missbräuchlich verwenden wollte? Was wäre, wenn ein Kill-Switch eingebaut wäre? Ist das wirklich möglich oder zu verhindern?

Jeder, der sich etwas intensiver mit IT-Security beschäftigt, weiß, dass es nie hundertprozentige Sicherheit geben kann. Also wären solche Attacken theoretisch doch möglich. Wer dies so weit wie irgend möglich, ausschließen will, der muss den Sicherheitsprozess im Unternehmen betrachten. Ist er so gestaltet, dass er Missbrauch ausschließt, können auch solche vermeintlichen Sicherheitsgefahren verhindert werden: Segmentierung und eine Firewall auf Applikationsebene, die jeglichen böswilligen ausgehenden Datenverkehr über IDS/IPS blockiert, sind hier die Mittel der Wahl. Eine Multi-Vendor-Umgebung und zusätzliche Sicherheitsmaßnahmen bieten Schutz vor einem Kill-Switch.

[2] https://www.welt.de/wirtschaft/article190034791/Huawei-Manager-zu-Spionagevorwurf-Das-hat-politische-Gruende.html
[3] https://www.golem.de/news/huawei-informatiker-gegen-ausschluss-aus-politischen-gruenden-1903-140259.html

2. Sicherheit in Kritischen Infrastrukturen

Betreiber Kritischer Infrastrukturen sind nach den beiden KRITIS-Verordnungen vom 3. Mai 2016 und 3. Juni 2017 in der Pflicht, die Einhaltung eines Mindeststandards an IT-Sicherheit nachzuweisen. Angesichts dieser Verpflichtung und der besonderen Verantwortung für den Betrieb ihrer für die Versorgung der Allgemeinheit in der Bundesrepublik Deutschlands wichtigen Anlagen, müssen sie ein besonderes Augenmerk auf diese zusätzlichen Maßnahmen legen. Dazu gehören Verschlüsselung, Monitoring oder auch Security by Design. Damit können sie die Netzinfrastruktur so sicher wie möglich gestalten und eben vor den beschriebenen – potenziellen – Gefahren schützen.

Und hier kommt telent – ein Unternehmen der euromicorn Gruppe ins Spiel. Zusammen mit dem Tochterunternehmen KORAMIS bietet telent umfassende Securitylösungen und Services, um diesen Schutz zu gewährleisten. Der Systemintegrator geht diese Aufgabe ganzheitlich an. Gerne empfehlen die telent-Experten beim Betreiben Kritischer Infrastrukturen eine Schwachstellenanalyse. Diese erkennt Angriffspunkte sowohl in der physikalischen Infrastruktur als auch in der organisatorischen Struktur der Securitystrategie eines Unternehmens. Die Experten analysieren dabei die Sicherheit der technischen Anlagen, Awareness der Mitarbeiter und Prozesse und bestimmen so den tatsächlichen Sicherheitsstand der IT- und Telekommunikationsinfrastruktur.

Für die Abwehr der potenziellen Gefährdungen durch Netzwerktechnik und deren Software helfen u.a. Maßnahmen zur Systemhärtung. Gleichzeitig schützen sie vor Risiken, die Mitarbeiter oder Fremdfirmen durch Fehlverhalten
verursachen. Wie sehen die zusätzlichen Sicherheitsmaßnahmen im Einzelnen aus?

Die telent Security Guideline - (1. Maßnahme)

telent unterwirft die Produkte aller Netzgeräte-Hersteller einer gewissenhaften und genauen Überprüfung. Eine Checkliste enthält die technischen Anforderungen für die Netzwerk-Hersteller. Die Guideline ist herstellerunabhängig und gilt für Cisco, Huawei, Nokia oder andere Partner/Hersteller gleichermaßen. Die telent-Mitarbeiter arbeiten diese Liste Punkt für Punkt ab, bevor sie ein System in Betrieb nehmen und prüfen dabei bestimmte Sicherheitsfunktionen/-einstellungen. Dazu gehören Fragestellungen wie: Ist bzw. wird das Standardpasswort gelöscht, sobald das Gerät angeschlossen wird? Werden offene Ports deaktiviert und existiert eine Firewall-Matrix für das System? Untersucht wird auch, ob es spezifische Einschränkungen für die einzelnen Systeme gibt. Mit Hilfe der Checkliste können die Sicherheits-Experten die Komponenten so einstellen, dass sie Best Practice-Beispielen folgen.

Im Zuge der Anwendung dieser Guidelines führt telent bei allen Lieferanten eine Sicherheitsüberprüfung durch. Gefragt wird unter anderem danach, wie sie generell, auch intern, mit Securitythemen umgehen? Ist ein Secure Code Review fest verankert, wie wird in den Arbeitsprozessen die Sicherheit mitberücksichtigt? Zusätzlich gibt es Checklisten für einzelne Technologien wie Richtfunk, DWDM, Access- und Carrier-Systeme, mit ihren jeweils unterschiedlichen Anforderungen. Auch hier zielen die Checklisten wieder darauf, die Sicherheitseinstellungen über die Implementierung von Best Practice-Verfahren zu härten („secure hardening“). Die dabei verwendeten Vorgaben beruhen auf Erfahrungen von telent sowie auf denen der Hersteller. Maßnahmen wie das Abschalten ungenutzter Schnittstellen, das Verwenden der neuesten Systeme in der aktuellsten Softwareversion und auszuschließen, dass das Standardpasswort nicht voreingestellt ist, sind Bestandteil der Überprüfung geworden,

nachdem den telent-Mitarbeitern immer wieder aufgefallen war, dass hier ein Bedarf ist. Sie achten auch darauf, wie das System in Betrieb genommen werden soll und welche Funktionen es hat. Diese Checklisten sind auf die jeweiligen Systeme spezifisch angepasst. Die meisten Fälle, die in der Checkliste festgehalten sind, kreisen um die Themen Standardpasswort, offene Kommunikationsverbindungen sowie ungenutzte Services, die bei unterschiedlichen Betriebssystemen mitlaufen, aber nicht benötigt werden.

Segmentierung der Netze - (2. Maßnahme)

telent setzt Firewalls ein, um die Netzwerke zu segmentieren. Heute geht man über das klassische Netzwerk-Firewalling auf Layer 3 hinaus und nutzt Next Generation Firewalls auf Layer 7 des OSI-Modells. Dabei kann die Software die Inhalte der Datenpakete sehr detailliert im Hinblick darauf, was tatsächlich auf Anwendungsebene passiert, prüfen. Über diesen Weg verstärkt telent die Sicherheit. Denn sollte ein Anbieter wie Huawei Datenabflüsse haben, fiele das dank dieser Firewalltechnologien auf, weil Traffic sichtbar würde, der bei klassischen Firewalls verborgen bliebe. Mit Segmentierung wird es möglich, den Netzverkehr dahingehend zu prüfen, ob es zu nicht erlaubten Verbindungen aus dem Unternehmensnetzwerk kommt.

Whitelisting und Sandboxing:

Gerade zielgerichtete Angriffe von Organisationen mit entsprechenden Ressourcen erfordern sehr ausgefeilte Sicherheitsstrategien. Maßnahmen zur Systemhärtung helfen, derartige Gefahren abzuwehren, und schützen gleichzeitig vor Risiken, die Mitarbeiter oder Fremdfirmen auch durch Fehlverhalten verursachen können. Bei dieser Systemhärtung geht es, vereinfacht gesagt, darum, Regeln festzulegen, wer auf welche Systeme Zugriff hat und wer nicht. Insbesondere muss definiert werden, welche kritischen Anwendungen in einer Sandbox („Sandkasten“) laufen sollen. Sandboxing steht für eine Technik, bei der Software innerhalb einer von den übrigen Systemressourcen isolierten Laufzeitumgebung ausgeführt wird. Alle Aktivitäten in diesem isolierten Bereich bleiben ohne Auswirkung auf die äußere Umgebung; anders herum haben Eindringlinge keine Chance, die Software in der Sandbox zu erreichen und Schaden anzurichten.

Die Multi-Vendor-Strategie (3. Maßnahme)

Ähnlich der Anfang März 2019 aktualisierten Vorgaben der Bundesnetzagentur (BNetzA) sollte jeder Betreiber Kritischer Infrastrukturen bei Planung und Aufbau von Kommunikationsnetzen darauf achten, dass er diese mit Netz- und Systemkomponenten unterschiedlicher Hersteller plant und betreibt. Dies kann für das Core- bzw. Access-Network unterschiedlich ausgestaltet werden. Ein solcher Multi-Vendor-Ansatz ist kein Ausdruck eines grundsätzlichen Misstrauens gegenüber einem bestimmten Anbieter, sondern eher Ausweis einer vorausschauenden Infrastruktur. Diesen Ansatz sollte jeder Betreiber Kritischer Infrastrukturen verfolgen, und zwar nicht nur, wenn er einem Hersteller nicht (mehr) vertraut. Die Architektur könnte z.B. so aussehen, dass das Unternehmen im Access-Netzwerk mit Huawei-Geräten und im Transport-Netzwerk z. B. mit denen von Cisco arbeitet. Das Design sollte ggf. so ausgelegt sein, dass Vendor-Wechsel in einzelnen Abschnitten möglich sind.

Die in den Medien immer wieder zitierten Schläfer-Programme lassen sich mit den bekannten Sicherheits-Technologien nicht aufspüren, da die Programme inaktiv sind, bis sie geweckt werden. telent empfiehlt hier den Stand der Sicherheitsmaßnahmen im Unternehmen im Rahmen des kontinuierlichen Verbesserungsprozesses zu untersuchen und so etwaigen Sicherheitsgefährdungen vorzubeugen. Monitoring ist eine äußerst wichtige Aufgabe in der Cybersecurity. Immer wieder müssen die Sicherheitsverantwortlichen untersuchen, ob die

verwendeten Methoden zur Überwachung des eigenen Netzwerks zeitgemäß sind. Sie sollten auch klären, ob das, was sie überwachen lassen, auch so funktioniert, wie es sollte. telent empfiehlt ein Sicherheits-Event-Management nach dem derzeitigen Standardverfahren SIEM (Security Incident Event Management). Alle sicherheitsrelevanten Ereignisse können dabei umfassend und übersichtlich überwacht werden.

3. Methodisch zu sicheren Netzen

Mithilfe der beschriebenen Methoden versetzt telent seine Kunden in die Lage, Prozesse und Infrastrukturen effizient und sicher zu vernetzen und den Weg in die digitale Zukunft erfolgreich zu gestalten. Betreiber Kritischer Infrastrukturen und Industrieunternehmen vertrauen auf unsere Expertise. Durch die Konzentration auf den Bereich KRITIS verfügt telent nicht nur über umfassende Praxiserfahrung als Systemintegrator, sondern ist auch der Spezialist für Planung, Aufbau und Betrieb sicherer Netze und Systeme.

Da telent die vermuteten Sicherheitsgefährdungen durch Huawei mit den eigenen Security Guidelines kritisch hinterfragt hat und keinerlei Beanstandungen ausmachen konnte, vertreibt, implementiert und betreibt telent auch die Lösungen für Telekommunikationsnetze der nächsten Generation. Durch die Securityaudits, persönliche Gespräche und Tests, haben wir ein Vertrauensverhältnis zu Huawei aufgebaut.

Am telent Hauptsitz in Backnang haben telent und Huawei ein dediziertes „Joint Innovation Lab“ eingerichtet. Hier werden die Systeme hinsichtlich Funktionen, Interoperabilität und Sicherheit umfangreich getestet. Das Lab bietet unseren Kunden einen bestmöglichen Service bei Hard- oder Softwareproblemen, Gewährleistungsfragen sowie Fragen zur allgemeinen Handhabung von Huawei Geräten. Zudem finden vor Ort Schulungen statt, um Mitarbeiter optimal für ihren Service beim Kunden vorzubereiten. Dieses Prinzip gilt nicht nur für die Huawei-Systeme sondern generell für die Systemtechnik von anderen Herstellern des telent-Portfolios.

Wir empfehlen daher nach heutigen Stand mit guten Gewissens die Geräte des Weltmarktführers und freuen uns auf Ihre Reaktionen auf dieses Whitepaper. Gerne stehen wir jederzeit für telefonische Auskünfte zur Verfügung.

Autor und Kontakt

Nico Werner
Head of Cybersecurity
telent GmbH - ein Unternehmen der euromicron Gruppe
Telefon: (07191) 900-0
E-Mail: info.germany@telent.de
Web: www.telent.de

Über den Autor:

Nico Werner begeisterte sich schon früh für Computer, insbesondere für die Absicherung von Computern und IT-Infrastrukturen.
Eine Ausbildung zum Fachinformatiker mit dem Schwerpunkt Cybersecurity rundete dieses Interesse ab. Das Thema der IT- und OT-Security prägte seine bisherige berufliche Laufbahn.

Seit 2012 hat er sich bei verschiedenen namhaften Konzernen dem Themenkomplex Cybersecurity angenommen u. a. bei Audi, SimonsVoss und NATEK Technologies. Seit Januar 2017 ist er federführend als „Head of Cybersecurity“ bei der telent GmbH tätig, getreu seinem Motto „Cybersecurity ist Chefsache“ mit dem Ziel: Die Bedeutung der Thematik den entscheidenden Stellen zu vermitteln und dafür Sorge zu tragen, dass die Umsetzung und stetige Verbesserung dieser vorangetrieben wird.

Er engagiert sich in den Gremien der Bitkom, des TeleTrust, des PMe.V. und der IEC 62443.
Zusätzlich verfügt Nico Werner über Zertifizierungserfahrung in vielen Bereichen, u. a. ISO 27001, BSI gemäß §8a BSIG (Auditieren von Betreibern Kritischer Infrastrukturen (KRITIS)).