TAGESSPIEGEL
BACKGROUND

„Open Ran ist nicht unsicherer als andere 5G-Systeme“

Politik und Wirtschaft setzen viel Hoffnung in offene Mobilfunkfunktechnologie im Radio Access Network-Bereich, das sogenannte Open Ran. Eine Studie des BSI hatte den Systemen jedoch im vergangenen Jahr hohe Sicherheitsrisiken bescheinigt. Doch die sind offenbar nicht nur leicht behebbar, sondern auch nicht größer als bei geschlossen Ran-Systemen.

von **Katharina Schneider**

veröffentlicht am 02.05.2022

Für Telekommunikationsunternehmen war es keine gute Nachricht: Im November veröffentlichte das **Bundesamt für Sicherheit in der Informationstechnik (BSI)** eine *Analyse (https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Studien/Open-RAN/Open-RAN_node.html;jsessionid=40577AE21274691C59D5E759062A6593.internet471)*, die sich mit den Risiken von *sogenannten Open Ran-Systemen (Open Radio Access Network) (https://background.tagesspiegel.de/digitalisierung/open-ran-was-kann-das-offene-mobilfunk-konzept)* beschäftigte. Das Ergebnis erscheint besorgniserregend: Die **offenen Systeme** würden derzeit **deutliche Sicherheitsrisiken** bergen, heißt es in der Studie, die federführend von der Dresdner Forschungseinrichtung Barkhausen Institut durchgeführt wurde. Von einer Vielzahl von Schnittstellen und Komponenten ginge eine mittlere bis hohe Gefahr aus. Die Telekommunikationsbranche, die sich von den offenen Systemen **mehr Flexibilität und geringere Kosten** erhofft, zeigte sich teilweise beunruhigt. Kein Wunder: Die Studie beschäftigte sich nur mit

Systemen der sogenannten **O-Ran Allianz**, einer von den großen Netzbetreibern und Vertretern *aus IT-Branche und Wissenschaft getragenen Industrieallianz (https://www.o-ran.org/)*.

Nicht nur die Unternehmen setzen auf Open Ran. Auch die **Politik** sieht in der Technologie eine Möglichkeit, sich **unabhängiger von den chinesischen System-Anbietern** für die für Mobilfunk notwendigen **Radio Access Networks (Ran)** zu machen. Denn die derzeitig eingesetzten Systeme sind alle geschlossen, insgesamt fünf Hersteller gibt es. Darunter die europäischen Unternehmen **Nokia** und **Ericsson**, den koreanischen Konzern **Samsung** und die chinesischen Hersteller **Huawei** und **ZTE**.

Nicht nur könnte man sich mit offenen Systemen unabhängiger machen, auch ein **Wettbewerbsvorteil** für Europa wird von Open-Ran-Anhänger:innen in Aussicht gestellt. Daher steckt man auch viel Geld in die Technologie: **Zwei Milliarden Euro** sieht das Konjunkturpaket der Bundesregierung für die Weiterentwicklung der Open-Ran-Technologie vor. Doch was, wenn die Systeme zwar Unabhängigkeit bringen, am Ende aber gar nicht sicher sind? Steckt der Bund dann Milliarden in eine Technologie, welche die IT-Systeme in der Bundesrepublik unsicherer machen? Und das, obwohl man in Open Ran hauptsächlich eine Technologie für 5G und den Nachfolgerstandard 6G und derzeit **vor allem für den Einsatz in 5G-Campusnetzen**, also der Industrie und Wirtschaft, sieht?

„Offene Systeme sind oft sicherer"

Nein, sagt **Slawomir Stanczak** von der TU Berlin und Abteilungsleiter des Fraunhofer Heinrich-Hertz-Instituts (HHI). In einem *gerade fertiggestellten Whitepaper (https://arxiv.org/abs/2204.12227)*, das im Juni auf der European Conference on Networks and Communications vorgestellt wird, analysiert er gemeinsam mit andern Autor:innen, was dran ist an der BSI-Studie. Und **wie sicher oder unsicher Open Ran wirklich ist**. „Wir haben in unserer Forschung bisher nicht festgestellt, dass durch Open-Ran-Konzepte wie O-Ran große Sicherheitsprobleme entstehen", ist das Ergebnis.

„Ich habe mich über die BSI-Studie etwas geärgert, weil dort **nur auf Risiken eingegangen** und so den Menschen Angst gemacht wird", sagt Stanczak im Gespräch mit Tagesspiegel Background. **Traditionelle 5G-Systeme seien nämlich nicht unbedingt sicherer** als Open Ran. „Im Gegenteil: Offene Systeme sind oft sicherer und schaffen Vertrauen, eben weil man in sie

schauen kann. In ein geschlossenes System können Außenstehende nicht hineinschauen."

Natürlich gebe es durch die **größere Oberfläche des Systems** Open Ran auch eine größere Angriffsfläche, heißt es im Whitepaper. Aber man könnte Risiken mit mehreren Praktiken umgehen. Es sei wichtig, solche Sicherheitssysteme schon **in einem frühen Stadium** in ein System zu integrieren. Und weil Open Ran in der Entwicklung noch nicht so weit sei, könnte man „**Security by design**" schon jetzt integrieren. Das sei wesentlich effektiver als eine Integration zu einem späteren Zeitpunkt im Lebenszyklus einer Technologie. Auch die BSI-Analyse hatte es als einen der Hauptherde für Sicherheitsrisiken ausgemacht, dass sich der Prozess bisher nicht am Paradigma Security und Privacy by design orientiere.

Bei O-Ran Systemen gebe es mehrere Möglichkeiten für Angriffe, schreiben die Autor:innen in ihrem Whitepaper. Auch verschiedene Angreifer seien vorstellbar. Das könnten zum Beispiel **Outsider** sein, oder **Insider**, **User** oder auch **Cloud-Operator,** die eine **Kontrolle über die Cloud-Infrastruktur** hätten. Um Sicherheitsprobleme zu lösen, müssten bestimmte Sicherheitsaspekte angewandt werden.

Sicherheitsstandards sind unbedingt nötig

Zum einen bräuchte es **standardisierte Mechanismen** für die Sicherheit. So sei es zum Beispiel notwendig, eine eindeutige Definition eines klaren **Rechte- und Rollenkonzepts** in Bezug auf die Kommunikation der Interfaces und Services zu entwickeln. Außerdem könnte man konkrete Maßnahmen anwenden, zum Beispiel die des **Reports für Network Function Virtualization der European Union Agency for Cybersecurity Enisa**. Diese könnte komplett auf Open-Ran-Systeme übertragen werden. Auch fehle es in der Definition von O-Ran an verschiedenen Sicherheitsaspekten. Diese bräuchte es aber, um die Systeme zu zertifizieren. Stanczak kann sich vorstellen, dass das BSI die Zertifizierung von Open Ran-Systemen beauftragt, **der Tüv könnte sie dann vornehmen**. Außerdem könnten neue Player, unabhängige Unternehmen und Start-ups, die es für das neue Ökosystem, das durch Open Ran entstehen soll, dafür sorgen, dass die Systeme sicherer werden.

Besonders eine Komponente im System könnte für die Sicherheit sorgen, sagt Stanczak. „Bei Open Ran kommen die einzelnen Komponenten im

Allgemeinen von verschiedenen Herstellern, ein **Integrator** soll dafür sorgen, dass sie in ein kongruentes System integriert werden können. Und er **könnte am Ende dafür sorgen, dass das System sicherer wird.**“

Außerdem sollten gewisse Teile des O-Ran-Systems einer **obligatorischen Verschlüsselung** unterliegen, heißt es im Whitepaper. Die sei derzeit, wenn überhaupt, nur schwach vorhanden, was die Sicherheit des kompletten Systems schwäche. Auch frühere Ran-Systeme hätten bezüglich der Verschlüsselung ähnliche Probleme gehabt wie O-Ran jetzt, daraus hätten sich ebenfalls Sicherheitsrisiken ergeben. Durch stärkere Verschlüsselung habe man das Problem aber lösen können. Die Autor:innen empfehlen: Eine **starke Verschlüsselung sollte zur Pflicht werden**.

Auch um **Post-Quanten-Sicherheit** müsse man sich schon jetzt Gedanken machen. Es sollte aufgrund der dynamischen Entwicklung von Quantencomputern und ihrer Fähigkeit, aktuelle Sicherheitsmechanismen durchbrechen zu können, schon jetzt zumindest empfohlen werden, **Quanten-resistente Verschlüsselungssysteme** zu nutzen. „Sicherheitstechnisch bedeute das Post-Quanten-Zeitalter, dass alles, was wir bisher nutzen, dann nicht mehr sicher ist und **jede Verschlüsselung geknackt werden kann**“, sagt Stanczak.

Die meisten Open-Ran-Betreiber haben eigene Rechenzentren

Auch wichtig sei, die **Cloud-Umgebung** sicher zu machen. Denn natürlich entstünde durch die Tatsache, dass sich Open-Ran-Komponenten in der Cloud befänden, eine neue Bedrohung. Auch in der BSI-Studie empfahlen die Autor:innen, besonderes Augenmerk auf die Absicherung der Cloud-Infrastruktur zu legen. Besonders von der Annahme, dass **Cloud-Betreiber per se vertrauenswürdig** seien, sollte Abstand genommen werden, heißt es dort.

Ein Cloud-Provider, der die O-Cloud kontrolliere, habe die selben Möglichkeiten wie der Ran-Operator. In ihrem Whitepaper schlagen die Autor:innen zwei Maßnahmen vor, mit denen das Problem schon deutlich verkleinert werden könnte: Einmal müssten **Sicherheitsmaßnahmen** integriert werden, um sich gegen mögliche, nicht vertrauenswürdige Cloud-Betreiber zu wehren. Das könnte mit dem Konzept der **Trusted Execution Environments**, gesicherten Enklaven innerhalb einer Cloud, passieren. Zum anderen müssten **obligatorische Zugangskontrollen und**

Sicherheitsvoraussetzungen in die Definition von O-Ran aufgenommen werden, um die Sicherheit der Komponenten in der Cloud zu gewährleisten.

In der Praxis allerdings hätten, so die Autor:innen, die meisten Betreiber von O-Ran-Systemen **ihre eigenen Rechenzentren** und würden nicht auf externe Cloud-Anbieter setzen. Wenn das der Fall sei, könnte dem Cloud Betreiber auch das gleiche Vertrauen entgegen gebracht werden wie dem Ran-Operator, also demjenigen, der das System betreibt.

Machine Learning: Großes Potenzial und potenzielle Gefahr

Ein weiteres potenzielles Sicherheitsrisiko steckt laut Stanczak in **Machine Learning (ML)**. Die O-Ran-Allianz plant, mit Machine Learning bestimmte Netzwerk-Funktionen zu automatisieren und damit auch die Betriebskosten zu senken. Wegen ihrer „inhärenten offenen und modularen Natur" enthalte die Architektur aber bestimmte Herausforderungen bezüglich der Sicherheit. „Auch wenn in diesen datengetriebenen Ansätzen viel Potenzial steckt, können Entscheidungen zum Beispiel **durch kleine versteckte Änderungen in den Daten** beeinflusst werden", sagt Stanczak. „Dann können **neuronale Netze von Angreifern als Werkzeug eingesetzt** werden." Deshalb sei es wichtig, dass ein umfangreiches Wissen um die Art der möglichen Angriffe vorliege, wenn ML-Technologien in das System integriert werden.

Großes Potenzial für die Erhöhung der Sicherheit liege in **Explainable AI**. Denn „Erklärungen sind ein Schlüssel, um verschiedene Arten von Attacken zu identifizieren und sich gegen sie zu wehren". Auch die Analyse und die Lokalisierung der Ursache für einen Angriff seien so weit einfacher. Nicht zuletzt könnten ML-Technologien eingesetzt werden, **um Attacken überhaupt zu identifizieren.**

Insgesamt kommen die Autor:innen zu dem Schluss, dass die **Angriffsoberfläche bei Open-Ran-Systemen sehr viel klarer** sei als bei anderen Systemen. Das wiederum ermöglicht es, die Sicherheitsrisiken frühzeitig auszumachen und so zu effektiv verringern. „Es **spricht mehr für Open Ran als dagegen**", sagt Stanczak. „Wir würden mit der Technologie traditionelle Netze nicht ersetzen, sondern ergänzen und so mehr Flexibilität in gewissen Branchen bekommen." Es sei gut möglich, dass die Open-Ran-Entwicklung zu lange gedauert habe, um im öffentlichen 5G-Netz eine große Rolle zu spielen. „Anders sieht das aber bei **Campusnetzen** aus. Und **bei 6G, da bin ich mir sehr sicher, werden wir offene Systeme haben.**"