Digital Business University of Applied Sciences

Cyber- & IT-Security (M.Sc.)

Cloud Computing & Cloud Security

Wintersemester 2024/25

Cloud Everywhere

Aufgabe 1

Eingereicht von:
Elias Häussler

Matrikelnummer:
200094

Dozent:
Prof. Dr. Aymen Gatri

17. April 2025

Aufgabe

Warum ist die Cloud auch für Angreifer im Mobilfunknetzwerk interessant? Schaue dir den Talk *OpenRAN – 5G hacking just got a lot more interesting*[1] von *Karsten Nohl* bei der *MCH 2022* an und erkläre, welche Hauptangriffsvektoren Karsten identifiziert hat, wieso die Cloud für Mobilfunknetze relevant ist und welche Angriffe es gibt.

[1] https://media.ccc.de/v/mch2022-273-openran-5g-hacking-just-got-a-lot-more-interesting

Hauptangriffsvektoren

Der Betrieb moderner Mobilfunknetzwerke erfolgt heutzutage zumeist in der Cloud unter Zuhilfenahme verschiedener Virtualisierungstechniken wie *Kubernetes* und *Docker*. Karsten hat dabei verschiedene Angriffsvektoren identifiziert, die durch den Einsatz von Virtualisierung und Automatisierung entstehen können.

Ausbrechen aus virtualisierten Umgebungen. Durch den Einsatz privilegierter Container oder das Mounten des Docker-Sockets in Containern kann ein Angreifer aus einer virtualisierten Umgebung ausbrechen und Zugang zum Host-System erlangen. Privilegierte Container sind besonders anfällig, da sie einem Angreifer die vollständige Kontrolle über das Host-System ermöglichen können. Dies befähigt ihn, Daten auszulesen, Code direkt auf dem Host-System auszuführen und im schlimmsten Fall das gesamte System auszuschalten oder zu übernehmen.

Netzwerkzugriff über Docker-Container. Wenn Docker-Container die gleiche Netzwerkschnittstelle wie das zugehörige Host-System verwenden, eröffnet dies einem potenziellen Angreifer den Zugriff auf sämtliche Dienste im `localhost`. Wird ein solcher Docker-Container als Teil eines Kubernetes-Clusters betrieben, so ermöglicht die geteilte Netzwerknutzung beispielsweise Zugriff auf die Kubernetes-API[2]. Zudem kann ein Angreifer sämtlichen Netzwerkverkehr mittels `tcpdump` mitlesen.

Phishing & Social Engineering. Charakteristisch für moderne Mobilfunknetze ist die breite Automatisierung der dahinterliegenden Prozesse. Diese erfordern zumeist die Speicherung sensibler Daten, wie beispielsweise API-Schlüssel, in einer Weise, die es den Automatisierungsprozessen ermöglicht, sie auszulesen und einzusetzen. Mitarbeiter*innen, die für die Verwaltung dieser Daten verantwortlich sind, werden daher zunehmend zum Ziel von Phishing- und Social Engineering-Angriffen.

Relevanz der Cloud für Mobilfunknetze

Die Virtualisierung und Automatisierung von Mobilfunknetzen durch Cloud-Systeme bieten unterschiedliche Vorteile. Zum einen ermöglichen Cloud-Technologien **Flexibilität und Skalierbarkeit**, da Netzfunktionen in kürzester Zeit bereitgestellt und konfiguriert werden können. Hierbei spielen auch Technologien wie CI[3] und CD[4] eine wichtige Rolle, da sie Kontinuität in den Abläufen sicherstellen und im Vergleich zum klassischen Setup eine wesentlich flexiblere Alternative darstellen.

Cloud-Technologien sind zudem **kosteneffizienter** als der Einsatz klassischer Komponenten beim Aufbau von Mobilfunknetzen. Durch die Nutzung von OpenRAN[5] und Cloud-nativen Architekturen können die Abhängigkeiten von teuren Hardwarekompo-

[2] Application Programming Interface
[3] Continuous Integration
[4] Continuous Delivery
[5] Radio Access Network

nenten erheblich reduziert werden. Dies ermöglicht auch eine **dynamischere Ressourcenverwaltung**, bei der Mobilfunknetze flexibel auf plötzliche Lastspitzen reagieren können, indem Cloud-Ressourcen kostengünstig und skalierbar zugeschaltet werden.

Mögliche Angriffe auf Cloud-basierte Mobilfunknetze

Wie fast alle Cloud-basierten Netzwerke und Applikationen sind auch Mobilfunknetze, die auf Cloud-Technologien aufbauen, einer Vielzahl möglicher Angriffe ausgesetzt.

Ein schwerwiegendes Angriffsszenario stellen **DoS**[6]**/DDoS**[7]**-Angriffe** gegen Cloud-Infrastrukturen dar. Durch das gezielte Versenden massenhafter Anfragen kann es zu einer Überlastung einzelner Komponenten und im schlimmsten Fall zu einem Ausfall des gesamten Mobilfunksystems kommen. Diese Art des Angriffs ist nicht unüblich; DoS-Angriffe kommen in Cloud-Infrastrukturen heutzutage häufig vor und sind längst zum Alltag geworden.

Der eingangs erwähnte Angriffsvektor des Ausbrechens aus virtualisierten Umgebungen kann zu **Datenmanipulation und Spionage** führen. Dies ist im Kontext von Mobilfunknetzen besonders brisant, da die hier erhobenen Daten äußerst sensibel und schützenswert sind. Die Übernahme von Containern oder – im erweiterten Kontext – ganzer APIs kann daher ein erhebliches Sicherheitsrisiko darstellen und im schlimmsten Fall den Zugang zu kritischer Infrastruktur verwehren.

Verwundbar sind die Container auch, wenn sie nicht regelmäßig **Software-Updates und Sicherheitspatches** erhalten. Karsten Nohl weist in seinem Vortrag explizit darauf hin, dass jeder Docker-Container praktisch ein benutzerdefiniertes Betriebssystem darstellt, was *Patching*, *Hardening* und *EDR*[8] des Cloud-Systems erheblich erschwert. Bekannte Sicherheitslücken, die nicht rechtzeitig geschlossen werden, können daher ein Eingangstor für Angreifer darstellen.

[6] Denial of Service
[7] Distributed Denial of Service
[8] Endpoint Detection and Response

Eigenständigkeitserklärung

Ich trage die Verantwortung für die Qualität des Textes sowie die Auswahl aller Inhalte und habe sichergestellt, dass Informationen und Argumente mit geeigneten wissenschaftlichen Quellen belegt bzw. gestützt werden. Die aus fremden Quellen direkt oder indirekt übernommenen Texte, Gedankengänge, Konzepte, Grafiken usw. in meinen Ausführungen habe ich als solche eindeutig gekennzeichnet und mit vollständigen Verweisen auf die jeweilige Quelle versehen. Alle weiteren Inhalte dieser Arbeit (Textteile, Abbildungen, Tabellen etc.) ohne entsprechende Verweise stammen im urheberrechtlichen Sinn von mir.

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Alle sinngemäß und wörtlich übernommenen Textstellen aus fremden Quellen wurden kenntlich gemacht.

Die vorliegende Arbeit wurde bisher weder im In- noch im Ausland in gleicher oder ähnlicher Form einer anderen Prüfungsbehörde vorgelegt.

Erklärung zu (gen)KI-Tools

Verwendung von (gen)KI-Tools

Ich versichere, dass ich mich (gen)KI-Tools lediglich als Hilfsmittel bedient habe und in der vorliegenden Arbeit mein gestalterischer Einfluss überwiegt. Ich verantworte die Übernahme jeglicher von mir verwendeter Textpassagen vollumfänglich selbst. In der vorliegenden Arbeit habe ich **keine** (gen)KI-Tools eingesetzt. Ich versichere, dass ich keine (gen)KI-Tools verwendet habe, deren Nutzung der Prüfer bzw. die Prüferin explizit schriftlich ausgeschlossen hat.

Hinweis: Sofern die zuständigen Prüfenden bis zum Zeitpunkt der Ausgabe der Aufgabenstellung konkrete (gen)KI-Tools ausdrücklich als nicht anzeige-/kennzeichnungspflichtig benannt haben, müssen diese nicht aufgeführt werden.

Ich erkläre weiterhin, dass ich mich aktiv über die Leistungsfähigkeit und Beschränkungen der unten genannten (gen)KI-Tools informiert habe und überprüft habe, dass die mithilfe der genannten (gen)KI-Tools generierten und von mir übernommenen Inhalte faktisch richtig sind.

Münster, 17. April 2025

Elias Häußler