TelCrit

Cybersecurity Assessment Österreichischer Mobilfunknetze zur Verbesserung Kritischer Telekommunikationsinfrastruktur

Programm / Ausschreibung	KIRAS, F&E-Dienstleistungen, KIRAS-K-Pass-KMU Innovation AKUT KIA F&E Dienstleistungen (FED KIA_2023)	**Status**	laufend
Projektstart	01.04.2025	**Projektende**	31.03.2026
Zeitraum	2025 - 2026	**Projektlaufzeit**	12 Monate
Keywords	mobilfunk, telekommunikation, cybersicherheit, kritische infrastruktur, notrufe		

Projektbeschreibung

Mobilfunknetze zählen in Österreich zu den wichtigsten digitalen Kommunikationsmedien und sind sowohl für private und geschäftliche Verständigung, als auch in Krisen und Notsituationen unabdingbar.
Zum Schutz unserer kritischen Infrastruktur ist Cybersicherheit für den Betrieb robuster und widerstandsfähiger Netze von zentraler Bedeutung.

Die Abschaltung von 3G-Netzen und der vollständige Übergang zu 4G/5G bietet aufgrund verbesserter Sicherheitsmechanismen das Potential, die allgemeine Cybersicherheit im Mobilfunkbereich zu verbessern.
In der Praxis sind viele dieser verbesserten Mechanismen jedoch Konfigurationsabhängig, und nicht zwingend bei allen Providern aktiv, was substantielle Auswirkungen auf die Kommunikationssicherheit haben kann.
Neue Technologien (4G/5G) bergen zusätzliche Risiken durch mögliche Fehlkonfigurationen, da die Verantwortlichen mit der Technologie noch nicht vertraut sind und diese oft unter großem Zeitdruck eingeführt werden.
Nachlässig konfigurierte 4G/5G Netze können dadurch sogar unsicherer sein als Netze früherer Generationen (2G/3G).

Veraltete oder unsichere Konfigurationen werden aus Provider-Sicht oft nicht unmittelbar entfernt, da jede Konfigurationsänderung potentiell neue Kundenprobleme verursachen kann.
Für Kund:innen ist es in der Regel nicht einsehbar, über welches Protokoll (z.B. VoLTE, VoWiFi, RCS) eine SMS-Nachricht oder ein Anruf terminiert wurde bzw. welche konkreten Sicherheitsparameter (z.B. Verschlüsselungs- oder Key-Exchange Algorithmen) beim aktuellen Mobilfunkprovider verwendet werden. Da diese Verbindungsparameter vor Nutzer:innen verborgen sind, fehlt es an Cybersecurity-Sichtbarkeit und -Bewusstsein.

Aus diesem Grund wollen wir für mehr Transparenz hinsichtlich verwendeter Technologien und Sicherheitsparameter sorgen.
Unsere vergangenen Publikationen haben gezeigt, dass schwere Security-Schwachstellen in komerziellen Mobilfunknetzen existieren, von denen leider auch österreichsiche Provider betroffen waren.
Um derartige Fälle in Zukunft zu vermeiden und österreichische Mobilfunknetze noch sicherer und robuster zu machen, führen wir im Zuge dieses Projekts eine Marktweite Sicherheitsstudie durch, die sich auf die Sicherheitseinstellungen der

Funkverbindungsschicht (VoLTE) sowie neue 4G/5G-Messaging-Protokolle (VoWiFi und RCS) konzentriert. Die Ergebnisse sollen der RTR (Bedarsträger) helfen, Provider zur Verbesserung ihrer Sicherheitskonfigurationen zu bewegen, während kritische Lücken im Rahmen eines Responsible Disclosure Verfahrens gemeldet werden.

Abstract

Mobile networks are one of the most important digital communication channels in Austria and are indispensable not only for private and business communication but also in crises and emergency situations. To protect our critical infrastructure, cybersecurity is of central importance for the operation of robust and resilient networks.

The shutdown of 3G networks and the full transition to 4G/5G offers the potential to improve the cybersecurity in mobile communications due to enhanced security mechanisms. However, in practice, many of these improved mechanisms depend on configuration and are not necessarily active at all major providers, which can have substantial effects on communication security. New technologies (4G/5G) also carry additional risks due to potential misconfigurations, as the responsible technicians may not yet be familiar with the technology, which is often introduced under significant time pressure. Poorly configured 4G/5G networks can, therefore, be even less secure than networks of earlier generations (i.e., 2G/3G).

Outdated or insecure configurations are often not immediately removed from a provider's perspective, as every configuration change can potentially cause new customer issues. For customers, it is generally not visible which protocol (e.g., VoLTE, VoWiFi, RCS) is used to terminate an SMS message or a call, nor which specific security parameters (e.g., encryption or key exchange algorithms) are used by the current mobile provider. Hiding connection parameters from users through the simplest possible user interfaces inevitably leads to a lack of visibility and awareness.

For this reason, we aim to increase transparency regarding the technologies and security parameters in current use. Our past publications have shown that serious security vulnerabilities exist in commercial mobile networks, unfortunately affecting Austrian providers as well. To avoid such cases in the future and to make Austrian mobile networks even more secure and robust, we are conducting a nationwide security study as part of this project, focusing on the security settings of the radio communication layer (VoLTE) as well as new 4G/5G messaging protocols (VoWiFi and RCS). The results are intended to help the RTR (the regulatory authority) push providers to improve their security configurations, while critical vulnerabilities will be reported through a responsible disclosure process.

Projektkoordinator

- SBA Research gemeinnützige GmbH

Projektpartner

- Kibosec GmbH
- Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH)