Success Story

Vulnerabilities in WhatsApp

How SBA-K1 NGC Helps Companies Manage Digital Risks

A team from SBA-K1 NGC, consisting of researchers from **SBA Research** and **the University of Vienna**, has identified a large-scale privacy and security vulnerability in the globally used messaging service **WhatsApp**—once again demonstrating how independent IT security research generates tangible value. WhatsApp uses a so-called "contact discovery mechanism" to find users via phone numbers. The research findings showed that this mechanism could be abused to query **more than 100 million phone numbers per hour** and ultimately identify **around 3.5 billion WhatsApp accounts** worldwide.

Why This Matters for Companies: Concrete Benefits and Applications

Companies face the challenge of providing not only functional but also trustworthy systems. The research from SBA-K1 NGC shows that even large, established platforms like WhatsApp are not free of risks, and that independent auditing mechanisms are strategically valuable for uncovering hidden vulnerabilities before they become critical problems.

The successful collaboration between the University of Vienna, SBA Research, and Meta demonstrates that scientific research combined with a responsible disclosure process leads to constructive cooperation, the rapid closure of security gaps and the creation value for future development.

For companies, this means early risk identification, avoidance of regulatory and legal issues, and the development of a measurable advantage in terms of security. In addition, the publication of research results and their presentation at international security conferences (including the Network and Distributed System Security Symposium or the ACM SIGSAC Conference on Computer and Communications Security) establish valuable standards and best practices. These can be directly adopted by companies and integrated into their own security processes.

In their analysis, the researchers not only demonstrated the vulnerability but also showed which metadata—such as phone numbers, public keys, and timestamps—are used and how this data can be linked to past leaks.

"The work of SBA Research shows how important independent security research is for the early detection of systemic risks. The insights from the WhatsApp analysis provide valuable input for our own situational awareness and help to better identify similar vulnerabilities in other systems. The fact that the results have also received significant international attention demonstrates the high level at which SBA Research operates and shows that Austria,

through SBA Research, contributes to global cybersecurity," says Wolfgang Rosenkranz, Head of the National CERT Austria team.

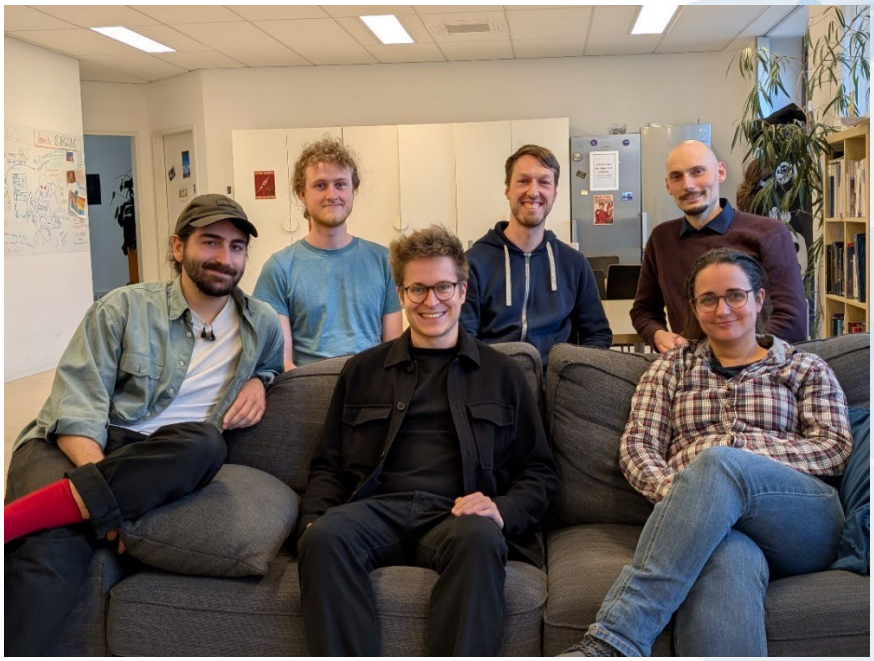

Figure 1: Researcher team, from left to right: Philipp Frenzel, Markus Maier, Aljosha Judmayer Maximilian Günther, Gabriel Gegenhuber, Johanna Ullrich © SBA Research, 2026

Conclusion

Within the framework of SBA-K1 NGC, research results directly impact companies. Our industry partners integrate new findings and testing methods into their tools, risk analyses, and services resp. are developing new ones, including specialized tests for enumeration vulnerabilities and enhanced privacy assessments.

This results in more secure products for their customers, clear competitive advantages, and new revenue opportunities in cybersecurity. The WhatsApp study is a prime example of how cutting-edge research from SBA-K1 NGC sustainably strengthens the innovative capacity and competitiveness of Austrian companies.

SBA Research gGmbH
Name: Gabriel Gegenhuber
Position: Researcher
E-Mail: ggegenhuber@sba-research.org

Partner
Name: Wolfgang Rosenkranz
Position: Team Lead CERT Österreich
E-Mail: rosenkranz@cert.at