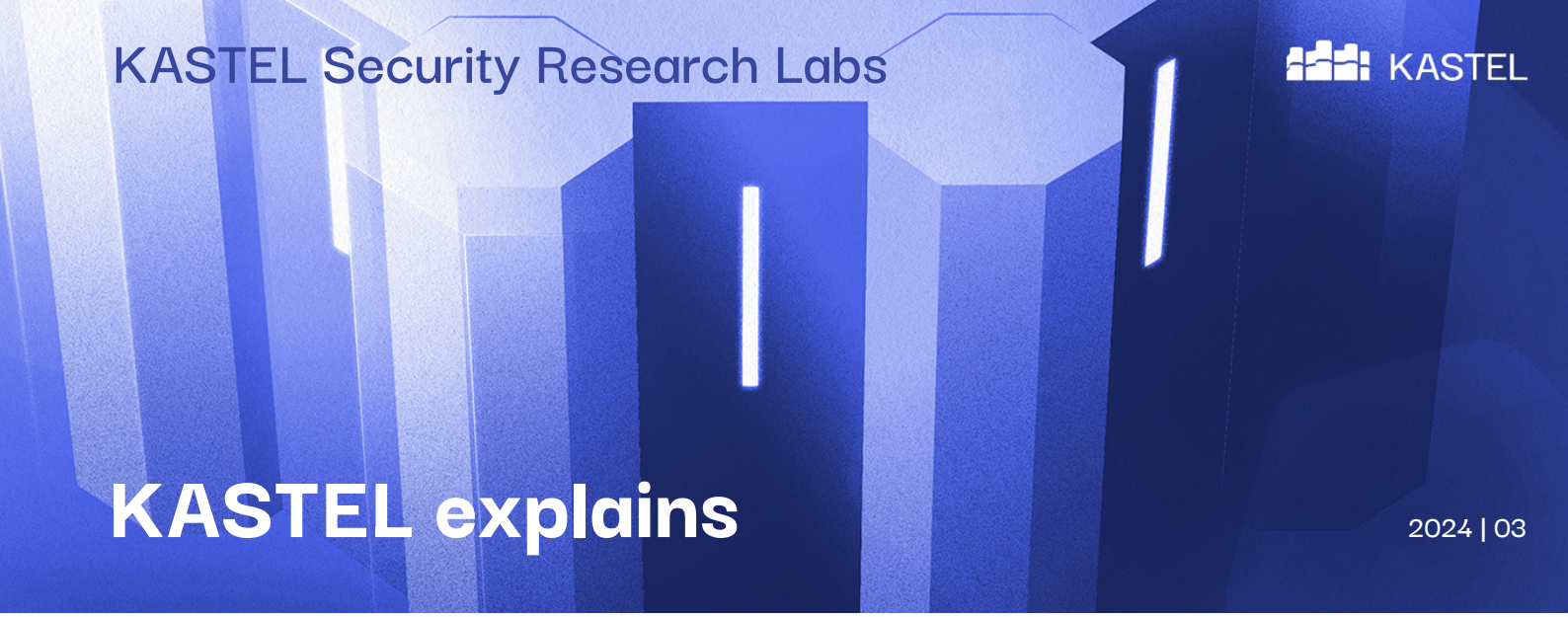

KASTEL explains

2024 | 03

Taurus Wiretapping Affair

Last week, Russia published a 40-minute-long recording of a Webex conference of high-ranking German officers discussing potential employment scenarios for Taurus cruise missiles. The wiretapping affair has led to heated debates. Experts at **KASTEL Security Research Labs** offer an assessment of current security-related questions.

Currently, it is speculated that an application error by one of the attendants enabled Russia to intercept the meeting. It this explanation plausible?

We have no detailed information on which vulnerability was exploited. According to statements by the Bundeswehr, an internally-operated Webex from Cisco was used. For this reason, we should not assume that a vulnerability on the side of external provides caused the issue. More so, the indication that a participant joined the meeting from an unsecured hotel network leads to the assumption that the problem lies here – in the failure to secure a network connection through encryption.

What could be the source of the security vulnerability?

In general, cloud-based conference systems such as Zoom, Teams, or Webex should be considered insecure if their implementations are not available as open-source. For this reason, open-source systems such as Jitsi, BigBlueButton, or Matrix, which is officially used by the Bundeswehr, should always be given priority to.

Nevertheless, given the circumstances of the case in question, we should not assume that a vulnerability or data leakage lies at the heart of the issue. It appears more reasonable to suggest that the failure to communicate by phone via a secured connection is to blame.

Can administrative bodies, research institutions, companies, or even private individuals trust in online conference systems to be secure?

Fundamentally, cloud-based conference sys-tems are always insecure in relation to their operators. Business secrets or any other sensible information should never be shared over these platforms. Open-source, self-operated, and encrypted

systems are always the better alternative. However, there are differences when it comes to the trustworthiness of the different providers. A person who uses Office 365 has already made the decision to trust the provider and will probably be unconcerned of recent events.

How can vulnerabilities be avoided in the future? What can we do to protect ourselves?

In general, we recommend to both keep systems up-to-date and avoid relying on cloud-based conference systems as often as possible. Self-operated systems that enforce encrypted communication are available for free and offer the same comfort functions as commercially-operated systems. It is important to mention, however, that there is always the possibility for new vulnerabilities to be found. In the concrete case, we are most likely dealing with an operating error. Avoiding these can be realized through better user interfaces, ruling them out completely is not possible, however.

What can researchers do to minimize risk in the future?

Particularly with regard to the usability of secure systems, there is a lot of work ahead of us. Evidently, we also need to further focus on how secure encryption can be implemented and how communication through networks and end systems can be secured. The case of the Taurus wiretapping affair appears to demonstrate that user mistakes can lead to vulnerabilities. Accordingly, we have to find solutions on how awareness for the issues can be increased as well as how proficiency in dealing with IT systems can be improved and systematically simplified.

www.kastel-labs.de