



Einladung zu einem Habilitationsvortrag

der Bergischen Universität Wuppertal

Die Fakultät für Elektrotechnik, Informationstechnik und Medientechnik lädt zur Teilnahme an folgender Vortragsveranstaltung mit anschließender Diskussion ein:

Es spricht

Dr.-Ing. Kai Gellert

Lehrstuhl für IT-Sicherheit und Kryptographie
Prof. Dr.-Ing. Tibor Jäger

über das Thema

Share with Care: Ende-zu-Ende-Verschlüsselung in Nextcloud brechen

Inhalt:

Nextcloud ist ein führender Cloud-Anbieter, der von mehr als 20 Millionen Nutzern zum externen Speichern und Teilen von Daten genutzt wird. Eine stark beworbene Sicherheitseigenschaft des Anbieters ist die Ende-zu-Ende-Verschlüsselung, welche die Sicherheit der verschlüsselten Daten garantieren soll, selbst wenn der Nextcloud-Server kompromittiert wurde.

In diesem Vortrag werden wir zunächst darstellen, wie Daten innerhalb des Nextcloud-Ökosystems verschlüsselt werden. Hierbei wird ein besonderes Augenmerk auf das Teilen von verschlüsselten Dateien (File-Sharing) gerichtet, welches das Erreichen einer Ende-zu-Ende-Verschlüsselung maßgeblich erschwert. Anschließend beschreiben wir eine Auswahl an praktischen Angriffen von Albert et al. (Euro S&P 2024) auf das Nextcloud-Protokoll, welche die Vertraulichkeit und Integrität der Dateien kompromittieren. Wir schließen den Vortrag mit einer Diskussion über die aktuellen Herausforderungen im Bereich des sicheren File-Sharings ab und geben einen Ausblick auf relevante Forschungsfragen zu diesem Thema.

T e r m i n : 12.11.2024, 15:30 Uhr

O r t: Bergische Universität Wuppertal
Campus Freudenberg, Hörsaal FZH 2