idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Press release

Bergische Universität Wuppertal
Katja Bischof
07/03/2023
http://idw-online.de/en/news817098

Research projects
Information technology
transregional, national

Daten speichern in der Cloud soll sicherer werden

Cloud-Dienste werden sowohl von privaten Anwender*innen als auch von Unternehmen genutzt, um Daten online zu speichern. Das Problem: Die Daten sind oft nicht richtig vor Zugriff von außerhalb geschützt, weil sie nicht ausreichend verschlüsselt sind. In dem Projekt „Entwicklung eines Post-Quanten-verschlüsselten Online-Speichers“ (PQDrive) arbeiten Forschende der Bergischen Universität Wuppertal in Kooperation mit dem IT-Security-Anbieter Tutao GmbH an neuen Ideen zur sicheren Speicherung und zum Austausch von Dateien.

Ziel ist eine Lösung zur verschlüsselten Cloud-Speicherung, um Angriffe auf die gespeicherten Daten in Cloud-Umgebungen und Datenverlust zu vermeiden. Prof. Dr.-Ing. Tibor Jager vom Lehrstuhl für IT-Security and Cryptography der Bergischen Universität und sein Team übernehmen im Rahmen des Projekts wichtige Forschungsaufgaben von der Erprobung kryptografischer Algorithmen bis zur ressourcenschonenden Speicherung verschlüsselter Daten.

Sichere Kommunikation im Internet unverzichtbar

Tibor Jager: „Sichere Kommunikation im Internet ist in unserem Lebensalltag, in Wirtschaft und Gesellschaft unverzichtbar. Sie wird durch kryptographische Algorithmen geschützt, die leider unsicher gegen Quantencomputer-Angriffe sind. Getrieben durch Fortschritte bei der Entwicklung von Quantencomputern müssen wir diese dringend durch sogenannte Post-Quantum Verfahren ersetzen, die auch im Zeitalter von Quantencomputern sicher sein können.“

Das neue Produkt soll eine Ende-zu-Ende-verschlüsselte Cloud-Lösung sein. Hierbei nutzen die Forschenden ein bereits im Rahmen eines Vorgängerprojektes entwickeltes kryptographisches Kommunikationsprotokoll, das neben zahlreichen Sicherheitsfunktionen auch Schutz vor möglichen, zukünftigen Angriffen durch Quantencomputer bietet.

Verfahren gegen Angriffe von Quantencomputern schon jetzt entwickeln

„Quantencomputer werden oft als Bedrohung gesehen, die vielleicht erst in 15 oder 20 Jahren wirklich relevant wird. Sie stellen aber schon heute eine Bedrohung dar, nämlich für Daten, die 15, 20 Jahre oder länger vertraulich bleiben sollen. Zum Beispiel in den Bereichen Gesundheitsdaten oder E-Government. Hier sollten schon heute Verfahren eingesetzt werden, die auch Angriffen von Quantencomputern standhalten können. Genau darum geht es im Projekt PQDrive“, so Jager.

Im Rahmen des Projektes wird das Protokoll für den Einsatz in einem Online-Speicher angepasst. Mit diesem Verschlüsselungsverfahren erhalten Endnutzer*innen und Unternehmen gleich zwei Vorteile: Zum einen behalten sie die Hoheit über ihre Daten, die derzeit zumeist nur mit lokaler Speicherung möglich ist. Zum anderen können sie die Vorteile von Cloud-Speichern – wie beispielsweise Erreichbarkeit, Kosteneffizienz und automatisches Backup – voll

ausschöpfen.

Das Projekt PQDrive wird vom Bundesministerium für Bildung und Forschung (BMBF) im Rahmen der Förderinitiative KMU-innovativ gefördert und hat ein Gesamtvolumen von 3,19 Millionen Euro. Knapp 640.000 Euro davon gehen an die Bergische Universität.

contact for scientific information:
Prof. Dr.-Ing. Tibor Jager
Lehrstuhl für IT-Security and Cryptography
E-Mail tibor.jager@uni-wuppertal.de

URL for press release: https://itsc.uni-wuppertal.de/de/