13. Karlsruher Tag der IT-Sicherheit

20.07.2023 | 14:00 – 18:40 Uhr

17:15 Uhr | Quantencomputer und Cybersicherheit: wie machen wir uns bereit?

Spätestens seit Shors Quantenalgorithmus zur Faktorisierung großer Zahlen ist bekannt, dass Quantencomputer irgendwann eine Gefahr für unsere Kommunikations- und Datensicherheit darstellen können. Heute gibt es bereits Cloud-Zugriff auf funktionsfähige kleinere Quantencomputer. Die Lösung ist quantenresistente Kryptographie: Kryptographische Verfahren für klassische Rechner, die robust gegen Angriffe durch Quantencomputer sind. Die Auswahl von Kandidaten für die Standardisierung solcher Verfahren ist derzeit in vollem Gange. Doch diese Verfahren basieren auf mathematischen Problemen, die deutlich jünger sind als das bereits durch Euklid untersuchte Faktorisierungsproblem. Gleichzeitig sind aktuell eingesetzte kryptographische Verfahren wie RSA oder ECDSA jedoch sicher gebrochen, sobald – oder falls – irgendwann ein ausreichend großer Quantencomputer existiert. Unter dem Stichwort Kryptoagilität wird deshalb empfohlen, Software bereits jetzt so aufzubauen oder zu modifizieren, dass kryptographische Algorithmen leicht austauschbar sind. Doch wie groß ist die Gefahr durch Quantencomputer? Inwiefern ist unsere Kryptographie betroffen, und ab wann müssen wir handeln? Sind symmetrische Verfahren bereits sicher gegen Quantencomputer? Und ist Kryptoagilität wirklich so einfach in der Praxis umsetzbar, oder ist dies vielleicht deutlich leichter gesagt als getan?

Dr. Carmen Kempka, WIBU-SYSTEMS, *studierte Informatik mit den Schwerpunkten Kryptographie und Quantencomputing an der Universität Karlsruhe (TH), heute KIT. Nach ihrer Promotion am KIT im Jahr 2014 im Bereich Kryptographie war sie für zwei Jahre als Postdoctoral Researcher in den Secure Platform Laboratories bei NTT in Japan. Es war und ist ihr stets ein Anliegen, eine Brücke zwischen Theorie und Praxis zu schlagen. Ende 2016 begann sie ihre Tätigkeit bei der WIBU-SYSTEMS AG, zuerst als Softwareentwicklerin. Heute arbeitet sie dort als Leiterin der Abteilung Corporate Technology an der Grenze zwischen Forschung und Entwicklung, betreut unter anderem die Einführung quantenresistenter kryptographischer Verfahren, und unterstützt mit ihrem Team ihre Kollegen in allen Fragen rund um Kryptographie und Product Security.*

www.tag-der-it-sicherheit.de

Profitieren auch Sie von den Erfahrungen anderer - wir freuen uns auf Ihr Kommen!