

Zitis: Staatliche Hacker sollen Verschlüsselung mit Quantencomputer knacken

[Originalartikel](#)

[Backup](#)

<html> <p class=„printversionback-to-article printversion-hide“><a href=„<https://www.heise.de/newsticker/meldung/Zitis-Staatliche-Hacker-sollen-Verschlueselung-mit-Quantencomputer-knacken-4175352.html>“>zurück zum Artikel</p><figure class=„printversionlogo“><img src=„<https://1.f.ix.de/icons/svg/logos/svg/heiseonline.svg>“ alt=„heise online“ width=„180“ height=„40“/></figure><figure class=„aufmacherbild“><figcaption class=„akwa-caption“><p class=„source akwa-captionsource“>(Bild: Shutterstock)</p></figcaption></figure><p>Die Bundesregierung hat ein 650 Millionen Euro schweres Förderprogramm für Quantentechnik aufgelegt. Ein Schwerpunkt ist der Sicherheitsbereich.</p> <p>Die vor einem Jahr eingerichtete „Zentrale Stelle für Informationstechnik im Sicherheitsbereich“ (Zitis) plant an ihrem künftigen Standort an der Universität der Bundeswehr München einen Quantencomputer zu nutzen, um klassische Verschlüsselungsverfahren einfacher brechen zu können. Dies geht aus dem Förderprogramm für Quantentechnik hervor, das die Bundesregierung am Mittwoch beschlossen hat.</p> <p>Das Bundeskabinett will so „die starke Position Deutschlands in der Forschung auf dem Gebiet der Quantenphysik ausbauen und den Weg zu quantentechnischen Anwendungen öffnen“. Dafür sollen bis zum Ende der Legislaturperiode 2022 rund 650 Millionen Euro für Forschung und Entwicklung bereit stehen.</p> <div class=„inread“/> <p>Mithilfe von Quantentechnik will die Regierung die „Sicherheit und technologische Souveränität“ gewährenleisten. Anwendungen mit Lichtteilchen hätten in diesem Bereich „enorme Auswirkungen“, heißt es in dem Papier [1]. Insbesondere sei die Datensicherheit betroffen.</p> <h3 class=„subheading“ id=„nav_bedeutende1“>Bedeutende Sicherheit</h3> <p>Die Quantenkommunikation gelte einschließlich eines darauf basierenden Schlüsselaustauschs einerseits als sicher, schreibt das Kabinett. Abhörversuche würden in Form von Datenverlusten sofort auffallen. So können „abhörsichere Kommunikationsnetzwerke“ eingerichtet werden. Andererseits können künftig Dritte imstande sein, mithilfe von Quantencomputern Algorithmen traditioneller Kryptosysteme wie RSA zu entschlüsseln.</p> <p>Die <a href=„<https://www.heise.de/meldung/Zitis-Kernteam-der-staatlichen-Hackertruppe-steht-4095295.html>“>staatliche Hackerbehörde Zitis [2] soll einen Quantenrechner gemeinsam mit dem Forschungsinstitut „Cyber Defence (Code)“ nutzen. Die Bundeswehr-Uni in München habe bereits einen Kooperationsvertrag mit IBM abgeschlossen, um dort einen „Quanten-Hub“ zu etablieren. Diese Schnittstelle biete die Möglichkeit zum kontinuierlichen

Austausch zwischen den Bundesministerien für Inneres und Verteidigung, „da die Entschlüssung bestehender IT-Sicherungssysteme in beiden Ministerien große Bedeutung besitzt“. (Stefan Krempel) / ()<br class=„clear“/></p><hr/><p>URL dieses Artikels:
<small>

<http://www.heise.de/-4175352>

</small></p> <p>Links in diesem Artikel:
<small>

[1] https://www.bmbf.de/pub/BMBF_Fo__rderprogramm_Quantentechnologie_2018.pdf

</small>
<small>

[2] https://www.heise.de/meldung/Zitis-Kernteam-der-staatlichen-Hackertruppe-steht-4095295.html

</small>
<small>

[3] mailto:anw@ct.de

</small>
</p> <p class=„printversion__copyright“>Copyright © 2018 Heise Medien</p> </html>

From:
<https://schnipsl.qgelm.de/> - Qgelm

Permanent link:
https://schnipsl.qgelm.de/doku.php?id=wallabag:zitis_-staatliche-hacker-sollen-verschlüsselung-mit-quantencomputer-knacken

Last update: 2021/12/06 15:24

