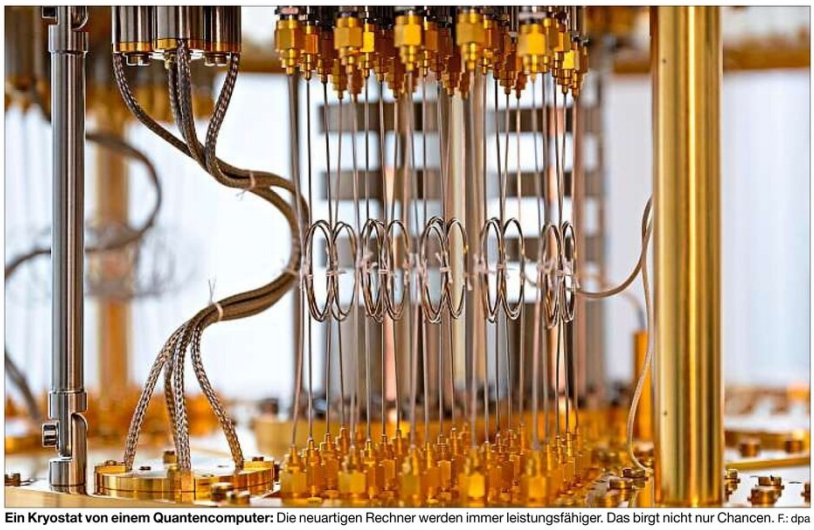
Der „Q-Day“ – das Ende aller Sicherheit

Leistungsfähige Quantencomputer können viele übliche Verschlüsselungen knacken. Stromnetze, Staatsgeheimnisse, das Finanzsystem – alles wäre verwundbar. Was bedeutet das für die Welt?

Von Felix Flesch



Ein Kryostat von einem Quantencomputer: Die neuartigen Rechner werden immer leistungsfähiger. Das birgt nicht nur Chancen. F.: dpa

Der sogenannte „Q-Day“ wird die Welt für immer verändern. Es ist der Tag, an dem der erste leistungsfähige Quantencomputer seinen Betrieb aufnimmt. Er wird eine Vielzahl von Verschlüsselungssystemen überwinden können. Die meisten mathematischen Rätsel, auf denen die digitalen Sicherheitsschlösser basieren, sind Experten zufolge für einen Quantencomputer kein Problem. Die Folgen könnten dramatisch sein.

Militär-, Staats- und Geschäftsgeheimnisse, das globale Finanzsystem, kritische Infrastruktur wie Stromnetze: Hacker hätten auf alles Zugriff. Die gute Nachricht ist, dass das Horrorszenario in der IT-Branche seit den 90er Jahren bekannt ist. Bei einem weltweiten Wettbewerb haben Kryptologen in den vergangenen Jahren neue Verschlüsselungstechniken gesucht, die auf heutiger Technik basieren und trotzdem quantensicher sind. Mit Erfolg. Es handelt sich um neue mathematische Probleme, von denen angenommen wird, dass selbst Quantencomputer diese nicht lösen können. Das heißt dann „Post-Quanten-Kryptographie“. Die vielversprechenden Verfahren können laut Wissenschaftlern bereits heute in die Netze integriert werden.

Hacker greifen heute Daten ab und bewahren sie auf

Damit sind wir bei den schlechten Nachrichten: Einerseits passiere dieser „Einbau“ viel zu selten. Viele Unternehmen haben von dem Thema noch nie etwas gehört oder sehen darin ein Problem der Zukunft. Wer weiß schon, wann der erste leistungsfähige Quantencomputer fertig ist? Allerdings kann das digitale Sicherheitsupgrade Jahre dauern. Wer auf der sicheren Seite sein will, sollte zeitnah loslegen.

Ein anderes Problem ist noch größer: Hacker greifen bereits heute Daten ab, die sie gar nicht entschlüsseln können, und bewahren sie auf. Denn sie wissen ganz genau, dass sie die Daten ab dem „Q-Day“ lesen können. „Store now, decrypt later“ („Jetzt speichern, später entschlüsseln“) heißt das in der Branche. Viele politische oder militärische Geheimnisse haben auch Jahre später enorme Sprengkraft. Ein solcher großangelegter Hackerangriff hat vor einem Jahr in den USA für Aufsehen gesorgt. Kriminelle besorgten sich Nachrichten von ranghohen Regierungsmitgliedern und bekannten Politikern. Auch mehrere Telekommunikationskonzerne waren betroffen. Die USA vermuten, dass China dahintersteckt. Ob die Hacker die Daten jetzt schon entschlüsseln können, ist offen. Klar ist, dass sie es irgendwann können werden.

Nur, wann ist irgendwann? Das Bundesamt für Sicherheit in der Informationstechnik (BSI) geht davon aus, dass der erste leistungsfähige Quantencomputer in höchstens 16 Jahren betriebsbereit ist. Ein Jahr vorher lag die konservative Schätzung noch bei 20 Jahren – innerhalb eines Kalenderjahres hat sich also die Prognose um vier Jahre reduziert. „Dies liegt daran, dass im Jahr 2024 ein wichtiger Meilenstein für diese Technologie erreicht wurde“, teilt das BSI auf Anfrage der Mediengruppe Bayern mit. Das zeigt, wie schnell es gehen kann.

Martin Bartenberger hilft Firmen beim Umstieg auf quantensichere Verschlüsselungen. F.: Flesch/OTH

Prof. Dr. Jürgen Mottok (OTH Regensburg) forscht, wie man die kritische Infrastruktur schützen kann.

Staatliche Institutionen sollen bis 2035 quantensicher aufgestellt sein. Das BSI überwacht den Prozess. In der Privatwirtschaft ist das Thema noch nicht wirklich angekommen. Das zeigt eine BSI-Umfrage. Von 150 Firmen und Organisationen, die angeschrieben worden sind, haben nur 28 geantwortet. Und die große Mehrheit rechnet nicht damit, Quantensicherheit zu erreichen, bevor die Vertraulichkeit ihrer Daten verletzt wird.

„Es ist oft so, dass für Unternehmen und Organisationen die Probleme der Gegenwart eine viel größere Rolle spielen“, sagt Martin Bartenberger. Der IT-Fachmann aus Thyrnau (Landkreis Passau) berät Firmen beim Umstieg auf quantensichere Verschlüsselungstechniken. Er arbeitet unter anderem für Signal. Der Online-Messenger aus den USA ist ein Vorreiter, was „Post-Quanten-Kryptographie“ angeht. Auch Apple und viele gängige Browser haben sich schon aufs neue Zeitalter eingestellt. Einige Nutzer kommunizieren post-quanten-verschlüsselt, ohne es zu wissen.

Bartenberger zufolge handelt es sich bei den neuen Verschlüsselungen nicht um komplett neue Sicherheitssysteme. „Stattdessen kombinieren wir die bewährten Verfahren mit den neuen. Wir bauen quasi ein zusätzliches Schloss ein“, erklärt er.

Allerdings könne das Jahre dauern. Besonders zeitaufwendig sei die „Inventur“. Bei dieser untersuchen IT-Experten wie Bartenberger, wo ein Unternehmen genau Verschlüsselungen einsetzt – sie schauen also, wo neue Schlösser integriert werden müssen. Sowohl Bartenberger als auch das BSI raten allen, die mit kritischen Informationen zu tun haben, jetzt mit der Umstellung anzufangen.

„Banken, Krankenhäuser, Versicherungen, große Industriebetriebe und alles Staatliche sollten schon heute tätig werden“, sagt Bartenberger. Für Privatleute bestehe keine Gefahr. „An seinem privaten Handy und Laptop muss man nichts ändern.“

Die Gefahr gehe künftig besonders von staatlichen oder staatsnahen Akteuren aus. Nicht jeder Hacker werde einen Quantencomputer besitzen. Man brauche die nötigen Ressourcen.

Bayern testet Einbau von quantensicheren Systemen

Bei der bayerischen Staatsregierung scheint das Thema angekommen zu sein. Zumindest hat der Freistaat als erstes Bundesland eine Landesbehörde für IT-Sicherheit errichtet, das Landesamt für Sicherheit in der Informationstechnik (LSI). Auch das LSI warnt mit Blick auf die „rasante Weiterentwicklung von Quantencomputern“ vor „erheblichen sicherheitsrelevanten Risiken“, wie es auf Anfrage unserer Zeitung heißt.

Damit die ganze Theorie auch in der Praxis ankommt, beteiligt sich das LSI mit der Ostbayerischen Technischen Hochschule (OTH) Regensburg und dem Zweckverband der Wasserversorgungsgruppe Laber-Naab an einem Projekt. Es geht darum, die Wasserversorgung quantensicher zu machen. Der Zweckverband soll eine Blaupause für ganz Bayern werden.

Prof. Dr. Jürgen Mottok ist an der OTH Regensburg der Experte auf diesem Gebiet. Er ist Forschungsprofessor für IT-Security und Leiter des Labors für Software-Engineering (Laboratory for Safe and Secure Systems) und arbeitet europaweit an Projekten zur „Posten-Quanten-Kryptographie“ mit. „Im Zentrum steht immer die kritische Infrastruktur“, sagt Mottok. Hier seien Deutschland und Europa besonders empfindlich. „Wenn wir nicht gut auf das Quanten-Zeitalter vorbereitet sind, könnten drei bis vier Tage nach einem Angriff auf unser Energienetz chaotische Zustände ausbrechen.“

Europa müsse sich quantensicher aufstellen. Das sei alternativlos. Denn der „Q-Day“ werde kommen. Die Frage sei nicht mehr ob, sondern nur noch wann.

Woran scheitern Quantencomputer noch?

Wer als erstes einen leistungsfähigen Quantencomputer entwickelt, hat die Technik der Zukunft in der Hand. Derzeit liefern sich weltweit etliche Firmen und Staaten ein großes Wettrennen. Wer sich am Ende durchsetzt, ist noch nicht klar.

In den USA sind vor allem große Spieler wie IBM, Google und Amazon vorne mit dabei. Dazu mischen in den USA, Kanada und Europa etliche Start-ups mit. In China finden vor allem staatlich getriebene Aktivitäten statt.

Auch in Deutschland und Bayern gibt es nennenswerte Fortschritte auf dem Weg zu Quantencomputern. Im Freistaat sticht das Munich Quantum Valley hervor, ein 2021 gegründeter Zusammenschluss von sieben großen Forschungseinrichtungen.

Ziel ist der Bau leistungsfähiger Quantencomputer. Woran scheitert das eigentlich noch? Pressesprecher Sascha Mehlhase zufolge gibt es drei Grundprobleme:

■ **Fehlerkorrektur:** „Quantencomputer machen Fehler. Das liegt in der Natur der Sache“, sagt Mehlhase. Das liege auch daran, dass die im Computer eingesetzten Qubits – diese können (in „Überlagerung“) die Zustände „0“ und „1“ zugleich annehmen – enorm empfindlich sind. Derzeit reiche ein Fehler, damit die komplette Rechnung verloren geht. Ziel ist es, dass Fehler in einzelnen Qubits kompensiert werden können.

■ **Skalierung:** Aktuell werde mit Quantencomputern gearbeitet, die über ein paar Dutzend oder mehrere Hundert Qubits verfügen. Perspektivisch sollen in den Computern etliche Tausend oder sogar Millionen Qubits eingesetzt werden. „Bis dahin dauert es noch ein bisschen“, sagt Mehlhase.

■ **Anwendungen:** So skurril es klingt: Noch ist vollkommen unklar, wofür Quantencomputer eingesetzt werden können. „Das ist vielleicht die größte Herausforderung.“ Es gibt aktuell wenige Bereiche, in denen die neuartigen Rechner – abgesehen vom Knacken von Verschlüsselungen – sicher einen Vorteil bringen. „Das könnte zum Beispiel beim Verständnis von Materialeigenschaften oder Molekülstruktureigenschaften der Fall sein.“

Das Munich Quantum Valley will bis 2030 Quantencomputer entwickeln, die „erste relevante Probleme“ lösen können. IBM will in wenigen Jahren den Punkt erreichen, an dem ein Quantencomputer Probleme gleich gut oder besser als ein normaler Rechner lösen kann. Das sind aber noch keine Computer, die alle bisherigen Verschlüsselungen knacken können. *ffl*

Die Machtdemonstration der ewigen Ski-„Göttin“

Lindsey Vonn pulverisiert die Konkurrenz in der ersten Abfahrt der Saison. Und das im Alter von 41 Jahren.

Von Christoph Lother

Die US-Amerikanerin Lindsey Vonn ist nun mit Abstand die älteste Weltcup-Gewinnerin der Alpin-Geschichte. Foto: Coffrini, afp

Lindsey Vonn grüßte noch schnell ihre Kritiker, Felix Neureuther kam aus dem Staunen gar nicht mehr heraus. Mit einem Fabellauf und einem gewaltigen Fingerzeig an die Konkurrenz ist Ski-Superstar Vonn in die letzte Saison ihrer Karriere gestartet. Die US-Amerikanerin fuhr in St. Moritz nicht nur zu ihrem ersten Weltcup-Sieg seit fast acht Jahren, sondern in einer eigenen Liga. Eine „Göttin“ sei die 41-Jährige, rief Neureuther begeistert.

Fast eine Sekunde legte die viermalige Gesamtweltcupsiegerin zwischen sich und die zweitplatzierte Österreicherin Magdalena Egger. „Es ist unfassbar“, sagte Ex-Skistar Neureuther als TV-Experte der ARD. „Das war mit das Beste, was ich jemals in meinem ganzen Leben gesehen habe.“ Und sie sei noch nicht mal zu 100 Prozent sauber gefahren, erklärte die strahlende Vonn selbst.

Im Ziel hatte sich die Abfahrts-Olympiasiegerin von 2010 zunächst in den Schnee fallen lassen. Als sie wieder aufgestanden war, gab sie einen kleinen Freudenschrei von sich und winkte in die Kamera. Als ihr im Interviewbereich später ein Handy gereicht wurde, begann sie zu weinen, weil ihr Vater am anderen Ende der Leitung vor Rührung weinte und sie ihn noch nie zuvor so emotional erlebt hatte. Sie habe all die Kritik als Motivation genommen, ließ Vonn noch einmal wissen. Bei ihrem Comeback im vergangenen Winter war sie von mehreren Ex-Skigrößen heftig angegangen worden. Spätestens mit diesem Sieg, dem ersten im Weltcup seit ihrem Triumph im schwedischen Are im März 2018, schlug sie nun eindrucksvoll zurück. Von der Rückkehrerin zur großen Favoritin für die Olympischen Spiele im Februar – so schnell kann es gehen.

Sie verschiebe Grenzen, sagte Neureuther über die nun mit Abstand älteste Weltcup-Gewinnerin der Alpin-Geschichte. Der frühere norwegische Skistar Aksel Lund Svindal, der seit Sommer zu ihrem Trainerstab gehört, fiel Vonn nach dem Rennen erleichtert um den Hals. Es scheint, als habe sich mit dem „Team Lundsey“ eine neue Traumkombination gefunden. Als könne sich Vonn ihren Wunsch von einer weiteren Olympia-Medaille tatsächlich noch erfüllen.

Der Konkurrenz dürfte Vonns denkwürdiger und historischer Auftritt acht Wochen vor den Winterspielen jedenfalls zu denken geben. Trotz ihres für eine Leistungssportlerin fortgeschrittenen Alters und einer Teilprothese im Knie, mit der sie inzwischen fährt, wirkt die in ihrer Karriere von schon so vielen Verletzungen gezeichnete Amerikanerin fit wie lange nicht – und demnach kaum zu stoppen. Auch am Samstag nicht? Sie sei selbst gespannt, sagte Vonn. *dpa*