digicert®

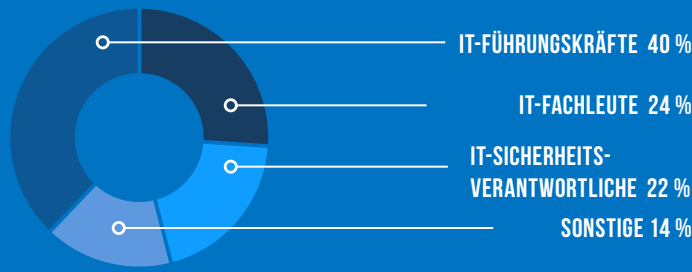
QUANTENCOMPUTER ALS CHANCE UND RISIKO:

DigiCert-Bericht zur PQC-Befragung 2019

METHODIK

DigiCert hat das Marktforschungsunternehmen ReRez in Dallas (Texas, USA) beauftragt, IT-Fachleute aus 100 deutschen Unternehmen mit mindestens 1000 Beschäftigten zu befragen.

Bei den Befragten handelte es sich um IT-Führungskräfte, IT-Sicherheitsverantwortliche und allgemeine IT-Fachleute.



Die Befragung konzentrierte sich auf vier wichtige Branchen:

Quantencomputer als Chance und Risiko

Im Januar 2019 stellte IBM den weltweit ersten kommerziellen Quantencomputer mit Quantenschaltungen vor: das IBM Q System One. Bis es Quantencomputer im Laden zu kaufen gibt, ist es zwar noch lange hin, aber viele Fachleute versprechen sich eine Menge von Quantencomputern und hoffen, damit Probleme lösen zu können, die aktuelle Computer schlicht überfordern. Maschinelles Lernen, medizinische Forschung und Teilchenphysik – das sind Beispiele für Gebiete, auf denen von Quantencomputern Großes erwartet wird.

Aber der durch Quantencomputer erwartete Leistungssprung birgt auch Gefahren. Die US-Behörde NIST und viele weitere Stimmen sagen voraus, dass Quantencomputer – vermutlich schon innerhalb der nächsten zehn Jahre – in der Lage sein werden, selbst die anspruchsvollsten Verschlüsselungsalgorithmen von heute zu knacken, was ernste Sicherheitsprobleme mit sich bringt.

Noch bevor es soweit ist, müssen IT-Fachleute daher neue Verschlüsselungsalgorithmen entwickeln, die Quantencomputern standhalten können. Man bezeichnet solche Algorithmen für die Zeit nach Einführung von Quantencomputern als Post-Quanten-Kryptografie (Post Quantum Cryptography, PQC). Aber PQC alleine wird nicht ausreichen.

Man denke nur an das Internet der Dinge, das IoT. PQC-Algorithmen sollen in der Lage sein, Angriffen durch Quantencomputer standzuhalten. Viele IoT-Geräte und -Anwendungen haben jedoch eine lange Lebensdauer, so dass ältere Produkte noch im Einsatz sein werden, wenn die ersten Quantencomputer zu einer Bedrohung werden. Dann werden diese einst sicheren Produkte zu einem Risiko. Ein Beispiel dafür sind Fahrzeuge mit Sensoren, Bordcomputern und Internetanbindung. Wenn bei ihrer Fertigung nicht schon heute Strategien zum Einsatz kommen, die auch im Quantenzeitalter Sicherheit garantieren, sind die Fahrzeuge später ungeschützt.

Um zuverlässigen Schutz zu gewährleisten, müssen sich Unternehmen daher schon heute mit der Bedrohung durch Quantencomputer auseinandersetzen. Aber wie können sie sichdarauf vorbereiten? Was weiß man in Unternehmen überhaupt über PQC?

Um Antworten auf diese und weitere Fragen rund um das Thema PQC zu finden, hat DigiCert, weltweit führender Anbieter von TLS/SSL-Zertifikaten und anderen Zertifikaten für Websites, Unternehmensanwendungen und den IoT-Markt, die PQC-Umfrage 2019 in Auftrag gegeben. Die Ergebnisse sind ein wahrer Weckruf für die Branche.

PQC ist bekannt, sorgt aber für Verunsicherung

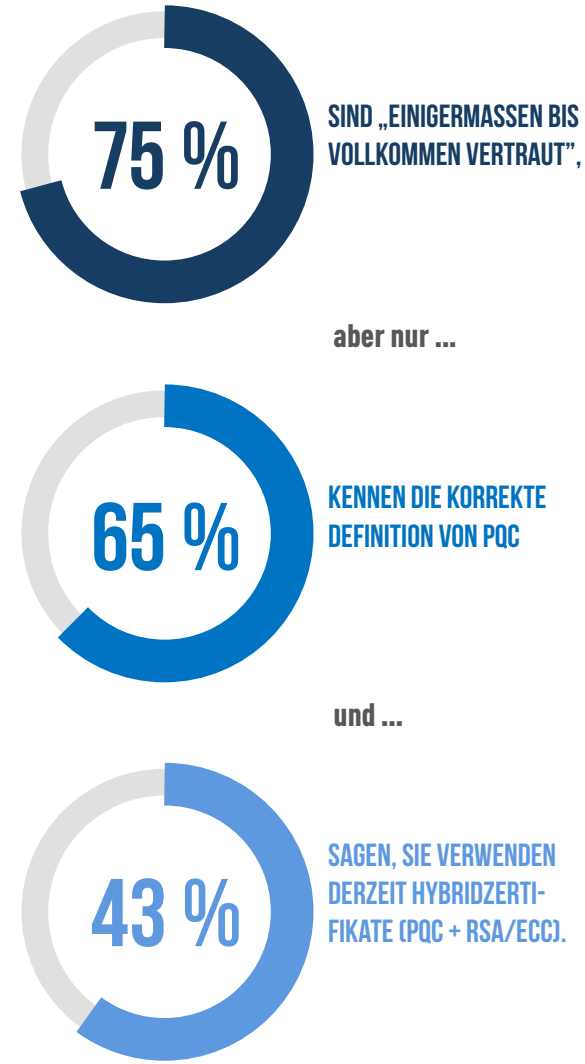
Den IT-Abteilungen in Unternehmen ist PQC in der Regel ein Begriff. Bei der Umfrage gaben drei Viertel an, dass sie „einigermaßen“ bis „vollkommen“ vertraut mit der PQC-Problematik sind. Aber wir wollten es genauer wissen und mit der nächsten Frage herausfinden, ob die Teilnehmer wirklich begriffen hatten, was es mit PQC auf sich hat. Nur knapp zwei Drittel kannten die korrekte Definition.

Noch bezeichnender: 43 Prozent gaben an, derzeit Hybridzertifikate (PQC + RSA/ECC) einzusetzen, was jedoch höchst unwahrscheinlich ist, denn PQC-Zertifikate gibt es derzeit nur für die allerersten Testfälle.

Überraschend ist das jedoch nicht, schließlich ist PQC neu und alle müssen sich noch mit dem Thema und den geeigneten Maßnahmen vertraut machen. Dies erinnert an eine Umfrage aus dem Jahr 2012, laut der mehr als die Hälfte der Befragten der Meinung waren, „stürmisches Wetter“ würde das Cloud-Computing beeinträchtigen[1]. Damals herrschte also trotz der Vertrautheit mit Cloud-Computing eine deutliche Verunsicherung, die allerdings nicht lange anhielt: Heute hat der Markt für Cloud-Computing einen Wert von 214 Milliarden US-Dollar weltweit.

Klar ist jedoch, dass Quantencomputer bei vielen im Bewusstsein angekommen sind und in aktuelle und zukünftige Planungen einfließen. Unsere aktuelle Studie untersucht außerdem, welche Maßnahmen Sicherheitsprofis für den Umgang mit der Bedrohung durch Quantencomputer für die Verschlüsselung ins Auge fassen.

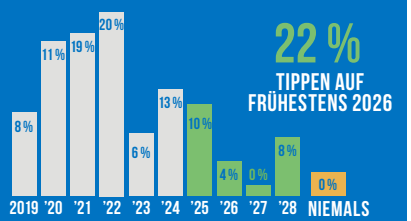
„Wir sind noch am Anfang der Diskussion, denn wir sind ja nicht als einzige betroffen. Wir besprechen mit Partnern und Zulieferern, wie wir aktiv werden und unsere Sicherheit stärken können. Und Quantenkryptologie ist eines der Themen, die wir dabei anschauen“, sagte ein IT-Sicherheitsmanager bei einem Finanzdienstleister.



1. „51% Of People Think Stormy Weather Affects ‘Cloud Computing’“, Business Insider, 30. August 2012

WANN

Wann werden Quantencomputer in der Lage sein, heutige krypto-grafische Algorithmen zu knacken?



22 % TIPPEN AUF FRÜHESTENS 2026

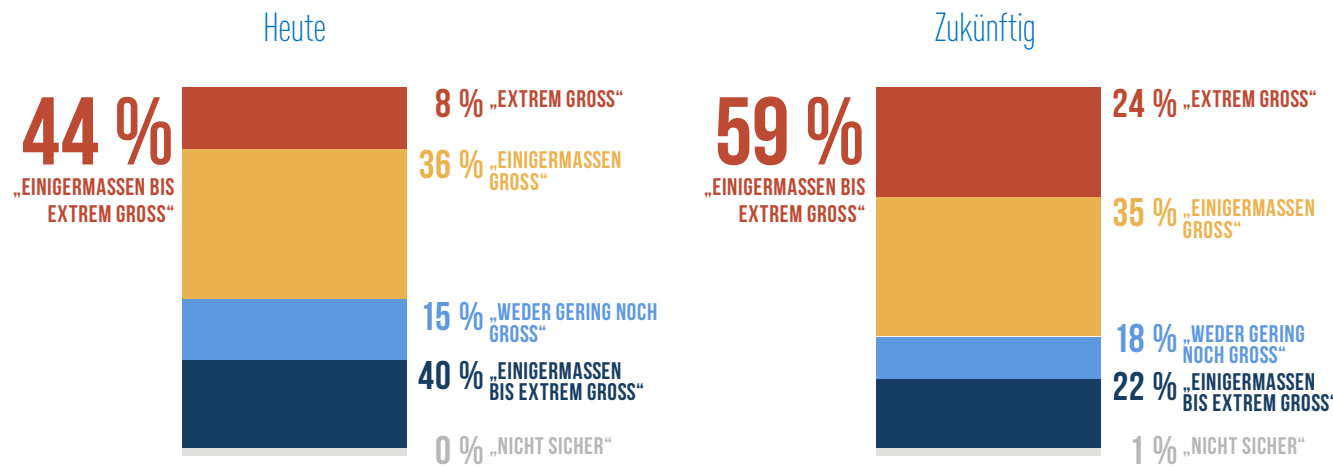
Fast alle Befragten gehen davon aus, noch immer in ihrem derzeitigen Unternehmen zu arbeiten, wenn die Gefahr aktuell wird.

7 VON 10

sagen, es ist einigermaßen bis extrem wichtig für die IT, sich mit quantensicheren Maßnahmen auseinander-zusetzen.

Die Bedrohung durch Quantencomputer ist real und nicht mehr fern

Trotz einiger Unklarheiten hat die IT klar erkannt, dass Quantencomputer eine Bedrohung für die Kryptografie darstellen. Knapp die Hälfte der Befragten (44 %) gibt an, dass Quantencomputer heute eine „einigermaßen" oder „extrem" große Bedrohung darstellen, und 59 % meinen, dass das zukünftig der Fall sein wird.

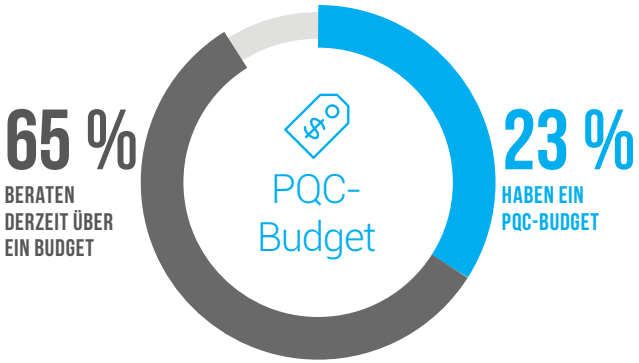


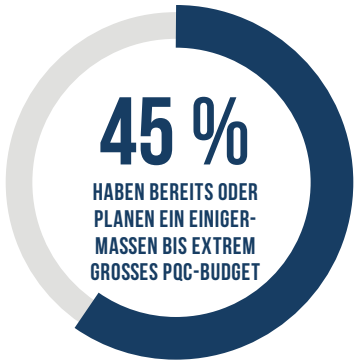
Und wann genau beginnt nach Ansicht der befragten IT-Fachleute die „Zukunft" im Zusammenhang mit PQC? Offenbar ist schon relativ bald. Der Mittelwert der Antworten auf die Frage, wann man PQC braucht, um die Gefahren durch Quantencomputer abzuwehren, lag bei 2022. Fast ein Viertel (22 %) meint, dass PQC erst 2025 oder später zum Einsatz kommen wird.

Die Bedrohung ist klar bekannt, der zeitliche Horizont überschaubar – da ist es kein Wunder, dass 66 Pro-zent der Umfrageteilnehmer es für wichtig halten, dass sich die IT in Maßnahmen zur Quantensicherheit einarbeitet. Aber was unternimmt die IT zur Vorbereitung, außer sich mit dem Thema vertraut zu machen?

Vorbereitung auf PQC

Unternehmen beginnen, sich auf PQC vorzubereiten: Fast ein Viertel hat ein PQC-Budget, und weitere 65 Prozent sind bereits dabei, eines einzurichten. Und wie groß sind diese Budgets? In fast der Hälfte der befragten Unternehmen sind die PQC-Budgets „einigermaßen“ bis „extrem“ umfangreich (45 %). Die bereitgestellten Gelder sind für Berater, Produkte und Personal vorgesehen.





Was konkrete Maßnahmen angeht, war (wenig überraschend) „die Lage verfolgen“ die derzeit wichtigste Taktik in der IT. Festzustellen, wie flexibel das Unternehmen in Sachen Kryptografie ist, folgte auf Platz 2. Hieran lässt sich ablesen, dass den Unternehmen die Notwendigkeit bewusst ist, schnell und effizient auf PQC-Zertifikate umzustellen, sobald diese verfügbar sind.

Zu den Top 5 der heutigen Maßnahmen gehörten außerdem die Risikoermittlung für das Unternehmen, die Einarbeitung in die PQC-Thematik und die Entwicklung von Best Practices für TLS.

DIE 5 WICHTIGSTEN MASSNAHMEN

1. **LAGE VERFOLGEN**
2. **KRYPTO-FLEXIBILITÄT**
   Wie flexibel ist das Unternehmen in Sachen Kryptografie aufgestellt?
3. **RISIKOEINSCHÄTZUNG**
   Bewertung des aktuellen Risikos für das Unternehmen und des akzeptablen Risikos
4. **EINARBEITUNG**
   Aufbau von Know-how zu PQC und Untersuchung der möglichen Auswirkungen
5. **BEST PRACTICES**
   Entwicklung von Best Practices für TLS im Unternehmen

Was zum Schutz vor dem Risiko durch Quantencomputer getan werden muss

IT-Fachleute sind sich des Risikos, das Quantencomputer für die Kryptografie darstellen, sehr bewusst. Zum einen machen sie sich Sorgen, dass die aktuelle Verschlüsselung nicht mehr sicher ist und vertrauliche Daten ohne Schutz sein werden. Zum anderen fürchten sie, dass die Industrie nicht rechtzeitig brauchbare Lösungen anbietet. Ähnliche Sorgen gibt es auch für IoT-Geräte. Sie sind zwar nach dem heutigen Stand der Kryptografie vor aktuellen Angriffsszenarios geschützt, werden mit den Möglichkeiten von Quantencomputern aber verwundbar sein. Für so langlebige Produkte wie Autos oder Bankautomaten wird das ein ernsthaftes Problem darstellen.

Die IT hat sich also dem Kampf um Sicherheit im Zeitalter von Quantencomputern verschrieben. Doch was sind die genauen Beweggründe? Neben der Stärkung ihrer Sicherheit versuchen Unternehmen, Zeit zu gewinnen, um sich mit den neuen PQC-fähigen Algorithmen vertraut zu machen. Außerdem muss dafür gesorgt werden, dass Nachrichten nicht mehr rückwirkend entschlüsselt werden können. Die IT macht sich bereits heute auf den Weg, weil die Verantwortlichen wissen, dass ein Wandel in der Kryptografie sehr schnell vonstatten gehen wird. Klar ist auch, dass es Unternehmen möglich sein muss, ihre alten Algorithmen schnell durch neue zu ersetzen, ohne den Netzwerkbetrieb zum Stillstand zu bringen.

All dies lohnt natürlich den Einsatz, aber es gibt einige Aspekte, die den Kampf erschweren. Das größte Problem ist – nach Meinung der von uns Befragten – das unzureichende Wissen der IT-Fachkräfte im Unternehmen. Verschärft wird dies dadurch, dass TLS-Anbieter aktuell keine PQC-Zertifikate im Angebot haben. Eine weitere häufig genannte Sorge betraf die Kosten für die Implementierung von PQC-Sicherheit.

Alles in allem sieht die IT die Probleme, die auf sie zukommen, realistisch. 46 Prozent meinen, es wird einigermaßen bis extrem schwer, ihre Verschlüsselung so aufzurüsten, dass sie auch gegen Angriffe von Quantencomputern schützt.

„Es wird früher oder später passieren. Und dann müssen wir vorbereitet sein“, sagt die IT-Leiterin eines Gesundheitsdienstleisters.

Empfehlungen von DigiCert

Quantencomputer gehören zu den drei Schlüsseltechnologien, die die Zukunft Ihres Unternehmens bestimmen.

Die Verheißungen dieser Technologie bringen aber Risiken für die Kryptografie mit sich. DigiCert, weltweit führend bei der Internet-Kryptografie, hat folgende Empfehlungen für Unternehmen, die jetzt mit der Planung von Strategien beginnen wollen, die ihre Sicherheit im Zeitalter von Quantencomputern gewährleisten.

RISIKO

Risiko kennen und ein Reife-gradmodell für die Quanten-kryptografie planen.

FÄHIGKEITEN

Bewusstsein für die Bedeutung von Krypto-Flexibilität für das Unternehmen erkennen und immer berücksichtigen.

BEST PRACTICES

Zusammen mit renommierten Anbietern Best Practices für digitale Zertifikate entwickeln und darauf achten, dass der Anbieter die PQC-Entwicklungen beobachtet, damit Sie mit den entsprechenden Produkten und Lösungen gewappnet sind. Änderungen brauchen meist Zeit für ihre Umsetzung, daher sollten Sie nicht zu lange abwarten, sondern das Thema Krypto-Flexibilität jetzt angehen.

Kontakt zu DigiCert

DigiCert, inc.
2801 North Thanksgiving Way
Suite 500
Lehi, Utah 84043

+41 22 518 9238
www.digicert.com

DigiCert ist ein weltweit führender Anbieter von renommierten digitalen Zertifikaten, die strengste Authentifizierungsanforderungen erfüllen, darunter vertrauenswürdige SSL-Zertifikate, Private- und Managed-PKI-Infrastrukturen und Gerätezertifikate für den neuen IoT-Markt. Seit unserer Gründung vor nahezu 15 Jahren setzen wir alles daran, unsere hervorragenden Produkte noch besser zu machen. Wir entwickeln kontinuierlich neue Lösungen für die Authentifizierung im Internet, die sich immer einfacher an die spezifischen Anforderungen unserer Kunden anpassen lassen. Dank der Erweiterung unserer eigenen Innovationsfähigkeit um die Erfahrungen und Talente von Symantec sind wir jetzt in der Lage, der Branche einen besseren Weg in die Zukunft zu weisen und das Vertrauen in Identitätsprüfungen und digitale Transaktionen zu stärken.