# 4 wichtige Schritte zur Vorbereitung auf Post-Quanten-Kryptografie

Durch die Fortschritte im Bereich des Quanten-Computings werden Kryptografie-Standards voraussichtlich bereits 2029 nicht mehr sicher sein.[1] Das bedeutet, dass eine gegen Quanten-Computing-gestützte Entschlüsselung resistente Kryptografie bald für sämtliche Unternehmen erforderlich wird. Angesichts dieser drohenden Gefahr sowie der bereits bestehenden Bedrohung durch „Harvest now, decrypt later (Jetzt sammeln, später entschlüsseln)"-Angriffe sollte Ihr Unternehmen die folgenden 4 wichtigen Schritte in Betracht ziehen, um sich auf die Post-Quanten-Kryptografie vorzubereiten.

## 1 Analyse der vertraulichen Daten Ihres Unternehmens und vorhandener kryptografischer Verfahren

Zur Vorbereitung auf die Post-Quanten-Kryptografie sollten Sie zunächst die aktuelle Anfälligkeit der Daten bewerten, die Ihr Unternehmen schützen muss.

Dies geschieht am besten durch die Zusammenstellung eines vielseitigen Teams (mit Mitarbeitenden aus den Bereichen Geschäftsbetrieb, Recht und Compliance, IT und anderen relevanten Abteilungen), das alle Zugriffswege auf diese Daten identifiziert und zurückverfolgt. Anhand dieser Erkenntnisse können Ihre Teams damit beginnen, Daten zu klassifizieren, die unter anderem jetzt sowie in naher oder ferner Zukunft als sensibel gelten.

Wichtig ist es auch, eine Bestandsaufnahme der derzeit in Ihrem Unternehmen verwendeten Verschlüsselungsprotokolle vorzunehmen und zu prüfen, welche Protokolle am dringendsten aktualisiert werden müssen, welche geändert werden können und welche aufgrund von Hardware- oder Softwarebeschränkungen unverändert bleiben müssen.

## 2 Ermitteln, welche Ihrer Vermögenswerte vorrangig zu behandeln sind

Nachdem Ihre Teams ein klares Konzept der sensiblen Daten Ihres Unternehmens haben, können Sie beginnen, die Assets zu priorisieren, die sofort geschützt werden müssen.

Eine gleichzeitige Sicherung sämtlicher Ihrer verschiedenen Assets ist weder praktikabel noch realistisch. Deshalb müssen Sie bei der Planung pragmatisch vorgehen und sich auf die bisherigen Erkenntnisse Ihrer Teams stützen, um sorgfältig abzuwägen, welche Assets und Systeme unverzüglich Priorität haben sollten und welche zu einem späteren Zeitpunkt berücksichtigt werden können.

1 Horvath, Mark. „Begin Transitioning to Post-Quantum Cryptography Now". Gartner, 30. Sept. 2024

## 3 Test neuer quantenresistenter Algorithmen in Ihrer Umgebung

Die meisten Compliance-Organisationen raten Unternehmen, so schnell wie möglich mit der Migration zu neuen Post-Quanten-Kryptografieprotokollen und -algorithmen zu beginnen, darunter auch die ersten finalen Standards, die im August 2024 vom National Institute of Standards and Technology (NIST) veröffentlicht wurden.[2]

Je früher Ihre Teams mit dem Testen von Algorithmen beginnen und Probleme beheben können, die eine erfolgreiche Migration Ihres Unternehmens verhindern könnten, desto besser sind Sie auf die bald verbindlichen Compliance-Anforderungen vorbereitet. Zudem können Sie so das Risiko von „harvest now, decrypt later"-Angriffen besser mindern.

Als Einstiegshilfe für Ihr Unternehmen beim Testen neuer quantenresistenter Algorithmen sollten Sie die Einführung oder ein Upgrade auf Red Hat® Enterprise Linux® 10 in Betracht ziehen. Dieses Betriebssystem (OS) enthält die erste Version quantenresistenter Algorithmen, – darunter OpenSSL, ML-KEM (FIPS 203) und ML-DSA (FIPS 204) – die Schlüsselaustausch, Verschlüsselung und Signierung ermöglichen. Weitere Funktionen sind für spätere Versionen geplant.

## 4 Start der umfassenden Migration und Aufnahme der Produktion

Dies ist zwar der letzte Schritt in diesem Prozess, aber die Implementierung neuer quantenresistenter Algorithmen ist der umfangreichste und komplexeste Teil.

Dieser Schritt sollte nicht als schneller Sprint zu sofortigen Ergebnissen betrachtet werden, sondern als nachhaltige Maßnahme, deren Ziel langfristige Vorteile sind.

Die Aktualisierung der einzelnen kryptografischen Algorithmen in Ihrer gesamten Umgebung lässt sich nicht sofort umsetzen, aber die in den vorbereitenden Schritten gewonnenen Erkenntnisse und festgelegten Prioritäten ermöglichen Ihrem Unternehmen nachhaltigen Erfolg.

Sobald Sie Änderungen an Ihren kryptografischen Protokollen vornehmen und quantenresistente Algorithmen in die Produktion integrieren, müssen Sie besonders auf sämtliche während der Testphase festgestellten Abhängigkeiten achten, um unbeabsichtigte Folgen oder Ausfallzeiten zu vermeiden.

### Noch heute mit der Vorbereitung auf Post-Quanten-Kryptografie beginnen

Hier erfahren Sie mehr darüber, wie Red Hat Enterprise Linux 10 quantenresistente Algorithmen integriert, mit denen Sie Ihr Unternehmen auf das Zeitalter der Post-Quanten-Kryptografie vorbereiten können.

2 „NIST Releases First 3 Finalized Post-Quantum Encryption Standards." National Institute of Standards and Technology, 13. Aug. 2024.



**EUROPA, NAHOST, UND AFRIKA (EMEA)**
00800 7334 2835
de.redhat.com
europe@redhat.com

**TÜRKEI**
00800 448820640

**ISRAEL**
1 809 449548

**VAE**
8000-4449549

facebook.com/redhatinc
@RedHatDACH
linkedin.com/company/red-hat

de.redhat.com