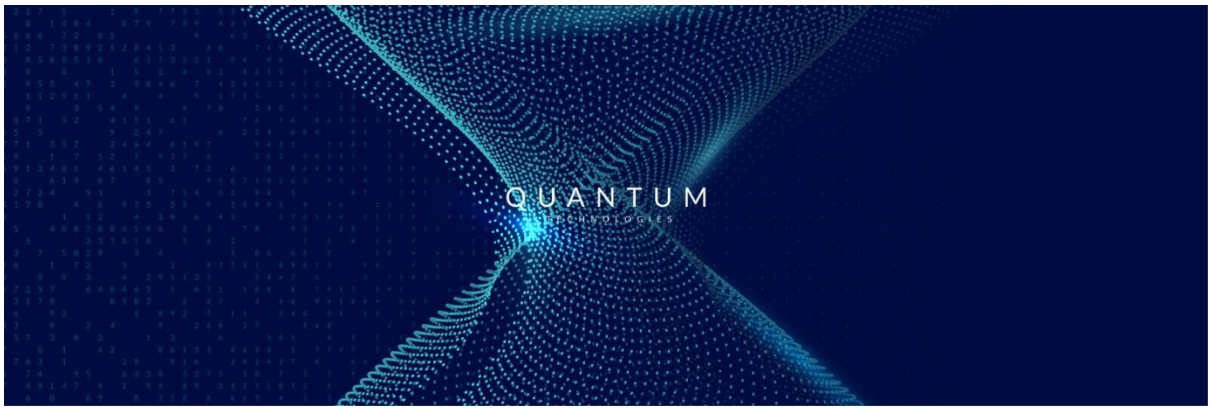
Kryptographie-Spezialisten – Schlüsselfiguren einer sicheren Post-Quanten-Welt

Geschrieben von Joshua Bucheli, Forscher und Redakteur, in Zusammenarbeit mit Xenia Bogolomec, Information Security Specialist und CEO der Quant-X Security and Coding und Peter Kosel, Gründer von cyberunity



"Cybersecurity" und "Kryptografie" mögen wie Tech-Jargon des 21. Jahrhunderts klingen, aber Datenschutz und Verschlüsselung sind keineswegs moderne Konzepte.

Vom alten mesopotamischen Handwerker, der sein Rezept für eine Töpferglasur verschlüsselte, um es vor Konkurrenten zu schützen, bis hin zur Enigma-Rotormaschine aus dem 20. Jahrhundert – die Verwendung von Chiffren zur Verschleierung von Informationen vor neugierigen Augen (Kryptographie) ist nichts Neues. Genauso zeitlos ist der Versuch, diese Codes zu "knacken" oder zu "entschlüsseln".

Im 21. Jahrhundert hat dieses Katz- und Mausspiel an Komplexität zugenommen, und wie bei Tom und Jerry sind beide Seiten immer mehr oder weniger auf Augenhöhe geblieben. Mit der Einführung von Quantencomputern, die eine unvergleichliche Rechenleistung aufweisen, wird sich das Spiel jedoch ändern.

Das Aufkommen von Quantencomputern wird sowohl neue Bedrohungen für die Cybersicherheit als auch neue Möglichkeiten für Jobsuchende im Bereich der Kryptografie mit sich bringen.

Ob die gesamte Cybersicherheitsbranche durch das Quantenzeitalter revolutioniert oder kompromittiert wird, hängt davon ab, ob die richtigen Spezialisten rechtzeitig hervortreten, um die Industrie bei der Anpassung auf quantensichere Verschlüsselung zu unterstützen.

Post-Quanten-Kryptographie: Ein neues Zeitalter der Cybersecurity

Die unübertroffene Rechenleistung von Quantenprozessoren wird es Computern ermöglichen, selbst die stärksten, konventionellen asymmetrischen Verschlüsselungen in

nur wenigen Minuten zu knacken. Damit wird die Grundlage der meisten Cybersicherheitssysteme obsolet und das Zeitalter der "Post-Quanten-Kryptografie" eingeläutet.

Das folgende Video bietet einen Crashkurs für alle, die sich für die Details interessieren, wie Quantencomputer Verschlüsselungen aufbrechen.

Das Wichtigste dabei ist, die Dringlichkeit dieses Themas zu verstehen. Laut Xenia Bogolomec, Informationssicherheitsspezialistin und Geschäftsführerin der Quant-X Security and Coding GmbH:

«Wenn Unternehmen in Zukunft die Vertraulichkeit der Daten, die sie heute über das Internet versenden, sicherstellen wollen, dann ist Post-Quanten-Kryptographie ein Schlüsselthema. Ein weiteres kritisches Thema (auch wenn Verifizierung nur durch NFC stattfindet, also ohne Internet) sind elektronische Pässe – hier werden private Schlüssel für Signaturen hinterlegt. Diese werden alle neu erstellt werden müssen, wenn Quantencomputer die Bühne betreten.»

Laut Experten wie Peter Shor und Schätzungen von IBM werden sicherheitsrelevante Vorfälle, aufgrund der Möglichkeiten, die sich aus Quanten-Computing für Hacker ergeben, bereits in den nächsten drei bis vier Jahren eine Realität.

Dieser Post-Quanten-Paradigmenwechsel in der Rechenleistung wird dramatische Auswirkungen auf die digitale Integrität von allem und jedem haben. Von der nationalen Sicherheit und elektronischen Ausweisen bis hin zu geistigem Eigentum und High-Tech-IT-Unternehmen – alle werden sich anpassen müssen.

Daher sind Post-Quanten-Kryptographie-Spezialisten, die die Zukunft der Cybersicherheit in einem Post-Quanten-Zeitalter mitgestalten können, unerlässlich.

Markante Entwicklungen und Arbeitgeber auf dem Gebiet der Post-Quanten-Kryptographie

Eine der am meisten erwarteten Entwicklungen auf diesem Gebiet ist die laufende Evaluierung von "quantensicheren" kryptographischen Methoden durch das NIST.

«Wenn dieser NIST-Standard in Kraft tritt, sind wir auf einem guten Weg, Systeme rechtzeitig vor der Ankunft von Quantencomputern zu sichern» sagt Xenia.

Allerdings sind regulatorische Standards nur ein Teil der Lösung. Es wird auch "Einsatz vor Ort" in Form von Algorithmen-Entwicklern, Krypto-Ingenieuren und Krypto-Beratern

brauchen, um die Welt auf den bevorstehenden Wechsel zur Post-Quanten-Kryptografie vorzubereiten.

Informatiker, die sich für solche Positionen interessieren, tun gut daran, ihre Jobsuche bei den Branchenführern in der Prozessorentwicklung wie Intel, CISCO, AWS, Infineon, IBM, Google und Microsoft zu beginnen.

Auch staatliche Nachrichtendienste sind auf der Suche nach Kryptographen und damit eine gute Anlaufstelle, wie die jüngste und durchaus sehenswerte Einstellungskampagne des BND zeigt: #followtheglitchkarnickel.

Organisationen wie PQ Shield und Almacrypt sowie Unternehmen wie Cybersec Innovation Partners (für diejenigen, die sich auf Public-Key-Infrastrukturen spezialisieren möchten) sind ebenfalls ideale Ansprechpartner für motivierte Interessenten.

Xenia lädt auch jeden ein, der daran interessiert ist, eine Karriere an der entstehenden Post-Quanten-Front der Cybersicherheit aufzubauen, sich bei ihrer Firma Quant-X Security & Coding zu bewerben, wenn eine Stelle oder ein Projekt auf der Firmen-Webseite ausgeschrieben ist.

Welche Hard Skills sollten Post-Quanten-Kryptografie-Spezialisten mitbringen?
Natürlich ist eine allgemeine Vertrautheit mit Cybersicherheitskonzepten eine Voraussetzung für eine Karriere in der Post-Quanten-Kryptografie. Aber es gibt bestimmte Fähigkeiten, mit denen sich angehende Kryptographen von der Konkurrenz abheben können.

Für Xenia ist der Fall klar: Wenn es um **Algorithmen-Entwickler** geht, braucht die Branche Leute mit den kombinierten Fähigkeiten eines Informatikers und eines Mathematikers.

«Personen, die in der Lage sind, theoretische Prinzipien aus diesen Disziplinen praxisorientiert auf Maschinen anzuwenden und Algorithmen in Programmen zu implementieren, sind besonders gefragt.»

Für Interessenten an **Crypto-Engineering** Positionen ist die Fähigkeit, kryptografische Lösungen zu implementieren, insbesondere im Hinblick auf Identity- und Access-Management, unerlässlich.

«Ein Crypto-Engineer muss nicht unbedingt wissen, wie ein diskreter Logarithmus algorithmisch implementiert wird. Aber er muss wissen, was ein Public-, Private-, und Session-Key ist, welche Kontexte welche Schlüssellängen erfordern und wie ein valider Zufallswert generiert wird», sagt Xenia.

Vor allem wollen Arbeitgeber also sehen, dass die Bewerber ein gutes Verständnis der Grundlagen der Kryptographie haben und dass sie über die notwendigen Kenntnisse und Fähigkeiten verfügen, um Timing- oder Zeit-Channel-Angriffe abzuwehren.

Zusätzlich zu diesen Fähigkeiten sollten angehende **Crypto-Consultants** auch die Fähigkeit mitbringen, effiziente und effektive Prozesse der System-Integration aufzusetzen, zu koordinieren und zu beaufsichtigen.

Vorteilhafte Qualifikationen und Erfahrungen:
Hochschulabschlüsse und Fachzertifikate in Mathematik, Informatik, Programmierung oder Ingenieurwesen legen eine gute Grundlage für eine Karriere in der Post-Quanten-Kryptografie.

Allerdings ist es die praktische Erfahrung, nicht Zertifikate oder Abschlüsse, die den Ausschlag für Kandidaten geben wird, sagt Xenia.

Für Positionen in der **Algorithmen-Entwicklung** werden Arbeitgeber nach Anwärter suchen, die in der Lage sind, eine effektive Qualitätskontrolle von Algorithmen durchzuführen. Der Nachweis starker analytischer Fähigkeiten, die Eignung zur regelmässigen Zusammenarbeit mit Teammitgliedern und eine nachweisliche Begeisterung für alles, was mit "Krypto" zu tun hat, sind entscheidend.

Die Teilnahme an Post-Quanten-Kryptographie-Konferenzen und die aktive Mitarbeit in der Fachgemeinschaft ist eine gute Möglichkeit, solche Erfahrungen zu sammeln und den Arbeitgebern zu zeigen, dass man mit Leidenschaft in Kryptographie involviert ist.

Personen, die aus netzwerkzentrierten IT-Bereichen kommen und Erfahrung mit Multi-Faktor-Authentifizierung oder der Erstellung von VPN-Modulen mitbringen – Netzwerk- und Firewall-Ingenieure, Identity-Access-Platform-Ingenieure oder Open-VPN-Programmierer – werden sich für **Crypto-Engineer** Positionen besonders eignen.

Was viele noch zu wenig auf dem Radar haben ist die Tatsache, dass Persönlichkeiten mit Erfahrung im IT-**Change Management** entscheidend sein werden, um den Übergang der Systeme von konventioneller zu Post-Quanten-Verschlüsselung zu ermöglichen.

Während Kryptographie-Kenntnisse ein Plus sind, ist es für diese Kandidaten wirklich wichtig, Erfahrung im **prozeduralen Zertifikatsmanagement** vorweisen zu können und die Standard Operating Procedures der **IT-Migration** zu beherrschen. Sie müssen in der Lage sein, Zertifikate in bestehenden Strukturen und Systemen zu identifizieren und zu ersetzen um sicherzustellen, dass diese auf dem neuesten Stand sind.

Persönlichkeit – über technisches Know-How hinaus:
Was die Persönlichkeit betrifft, so erfordern verschiedene Rollen unterschiedliche zwischenmenschliche Fähigkeiten. Wer zum Beispiel im Bereich der Algorithmik arbeiten möchte, muss in der Lage sein, in kleineren Teams von hochspezialisierten Experten zu arbeiten.

Crypto-Engineers, Crypto-Consultants und Change Manager hingegen werden regelmässig mit einer grösseren Anzahl von Teams interagieren müssen und brauchen deswegen auch stärkere integrative Fähigkeiten.

Xenia sieht das so: «Insgesamt ist die Post-Quanten-Kryptografie immer noch ein hochintellektuelles Feld. Der Auswahlprozess konzentriert sich mehr auf die technische Expertise als auf die Persönlichkeit - zumindest was die Algorithmen-Entwickler betrifft. Wenn es um Change Manager mit IT-Migrationserfahrung geht, dann sind hier, wie in vielen anderen Berufen auch, die zwischenmenschlichen Fähigkeiten viel entscheidender.»

Generell sollten diejenigen, die eine Karriere in der Post-Quanten-Kryptographie anstreben, sei es in der Algorithmik oder als Crypto-Consultant, ihre kritischen und analytischen Fähigkeiten, ihre Geduld und eine allgemeine Freude am täglichen Umgang mit komplexen Problemen betonen.

Es ist eine grosse Herausforderung, die Menschheit in ein sicheres Post-Quanten-Zeitalter der Cybersicherheit zu führen betont Peter Kosel, Founder & Talent Community Manager von cyberunity abschliessend. Weiter führt er aus:

«Es ist von zentraler Bedeutung, die richtigen Persönlichkeiten frühzeitig anzusprechen, kennenzulernen und zu pflegen. Wenn top Spezialisten erst dann angesprochen werden, wenn der Bedarf dringend ist, dann wäre das so, als würde man seine Kunden erst dann kontaktieren, wenn man den Umsatz braucht. Kann funktionieren, wird aber sehr eng.»