CODE-Jahrestagung 2022

Zusammenfassung zum Workshop QKD-gesicherte Netzinfrastruktur

Dieser Workshop widmete sich Fragestellungen, wie Quantum Key Distribution (QKD) in größere - auch bereits existierende - Netzinfrastrukturen so integriert werden kann, dass die Gesamtsicherheit dieser Infrastrukturen gesteigert wird. Der Workshop begann mit drei Vorträgen, welche dank der Referenten aus Industrie, Behörde und Universität verschiedene Perspektiven abdeckten. Danach folgte eine Paneldiskussion, bei der die verschiedenen Perspektiven rege diskutiert wurden

Im ersten Vortrag stellte Matthias Gunkel, Senior Architect bei der Deutsche Telekom Technik GmbH, das Projekt DemoQuanDT vor. In diesem Projekt entsteht zwischen Berlin und Bonn eine QKD-gesicherte Strecke. Die Strecke dient dem Forschungsbetrieb, daher entsprechen die Infrastrukturkomponenten der regulären Telekommunikationsinfrastruktur. Dies hat Einfluss auf das Design des Netzwerks, weshalb z.B. Software Defined Networking (SDN) verwendet wird, Schlüsselerzeugung und -nutzung separiert werden, sowie zwischen der Anwender- und der Betreiberinfrastruktur unterschieden wird. Als besondere Herausforderung für länderübergreifende QKD-Netze stellte der Referent das Zusammenspiel der internationalen und nationalen Controller sowie die Übergabepunkte an den Grenzen heraus.

Dr. Manfred Lochter, BSI, betrachtete das Thema QKD anschließend aus der Perspektive der Sicherheit. Das BSI arbeitet mit der Hypothese, dass 2030 leistungsfähige Quantencomputer verfügbar sein könnten, um klassische Kryptografie zu brechen. Die Lösungsmöglichkeiten QKD und PQC (Post-Quantum-Cryptography) beleuchtete er dabei aus Sicht der Sicherheitsbehörden. Das BSI legt ebenso wie seine Pendants in den USA, UK und Frankreich den Fokus auf die Migration zu PQC. Denn auch wenn QKD-Technologie heute grundsätzlich verfügbar ist, so fehlen insbesondere standardisierte Protokolle und zugelassene Geräte für den Einsatz im Hochsicherheitsbereich. Hierfür hat das BSI die Erstellung eines Protection Profiles im Rahmen der international anerkannten ETSI-Standards gefördert.

Im letzten Vortrag schlug Prof. Günter Schäfer, Institut für Telematik und Rechnernetze an der TU Ilmenau, die Brücke zu bestehenden VPN-Netzen. Am Beispiel eines Landesbehördennetzes stellte er dar, dass große moderne VPN-Netze hohe Anforderungen hinsichtlich Ausfallsicherheit, Flexibilität und Skalierbarkeit erfüllen müssen. Im Hochsicherheitsbereich kommt die Härtung der Systeme dazu. Aus dieser Perspektive plädierte er dafür, bei der Integration von QKD in VPNs möglichst Doppelarbeit zu vermeiden. Dies ist gegenläufig zu den bestehenden QKD-Standardisierungsansätze, die auf eine Separierung von QKD setzen. Im weiteren Vortrag ging er auf hybride Netze ein, bei denen nur Teilstrecken über QKD verfügen. Hier könnten QKD-Teilstrecken auch für Teilstrecken ohne QKD einen Sicherheitsgewinn bedeuten, wenn für die Schlüsselverteilung zwischen zwei Partnern grundsätzlich mehrere Pfade durchs Netz genutzt werden und hierbei auch QKD-Strecken mit genutzt werden.

Bei der abschließenden Paneldiskussion brachte Dr. Oliver De Vries, CTO von Quantum Optics Jena, die Perspektive eines Startups für QKD-Geräte ein. Dr. Kai Martius, CTO der secunet Security Networks AG, sowie Stefan Röhrich, Head of Certifications & Approval bei der Rohde

& Schwarz Cybersecurity GmbH, vertraten etablierte Hersteller von Verschlüsselungshardware. Matthias Görtz, CTO der BWI GmbH, sprach aus der Perspektive eines Infrastrukturbetreibers. Dr. Lucie Kogelheide, Fachexpertin Quantentechnologien bei der TÜV IT GmbH, erweiterte den Fokus auf die Implementierungssicherheit. Dr. Manfred Lochter vom BSI rundete die Diskussion erneut mit der Sicht einer Sicherheitsbehörde ab.

Unter der Leitung von Dr. Nils gentschen Felde, FI CODE, diskutierten die Teilnehmer lebhaft und auch das Publikum brachte sich aktiv mit Fragen und Kommentaren ein. Übereinstimmung gab es zu der Frage, ob die zusätzliche Komplexität durch QKD für den Sicherheitsgewinn gerechtfertigt sei. Die Panelteilnehmer waren darüber einig: Sobald andere Sicherheitsmechanismen durch verbesserte Quantencomputer in Bedrängnis gerieten, wäre kein Aufwand zu groß, um im Hochsicherheitsbereich geschützt kommunizieren zu können. Darum müsse die Vorbereitung auf künftige QKD-Netze bereits jetzt erfolgen.