Infotecs arbeitet an Quanten-Kryptografie-Verfahren

Berlin, 19. Juli 2017 – Der international agierende IT-Security und Threat Intelligence Anbieter Infotecs arbeitet an der Entwicklung einer zukunftssicheren Technologie des Quantenschlüsselaustauschs (Automatic System for Quantum Key Distribution). Dabei handelt es sich um eine technisch effiziente Lösung mit der höchsten Widerstandsfähigkeit zur Verschlüsselung von Daten-Traffic mit einem sehr hohen Aufkommen.

„Die Algorithmen, die bei der Public-Key-Infrastructure (PKI) eingesetzt werden, basieren auf der Rechenkomplexität einiger klassischer mathematischer Funktionen. Ein unerwarteter Durchbruch in der Mathematik oder eine sprunghafte Entwicklung der Computertechnik kann die gesamte asymmetrische Kryptographie in Frage stellen. Auch die PKI-Algorithmen, die sich heutzutage im IT-Bereich etabliert haben, verlieren kontinuierlich an Resistenz." – Dies ist ein Zitat aus einem Dokument von 2003, in dem Infotecs begründet, warum das Unternehmen in seinen Produkten von Anfang an auf die symmetrische Schlüsselverteilung setzt. Aktuelle Entwicklungen zeigen deutlich, dass die damals theoretische oben genannte Annahme bald zum Alltag wird. Denn der Wettbewerb hat bereits begonnen: Sowohl Geheimdienste, private, militärische als auch öffentliche wissenschaftliche Einrichtungen der ganzen Welt arbeiten an der besten Quantencomputer-Technologie. Die Experten vermuten, dass ein funktionierender Quantenrechner bereits bis 2025 oder eher gebaut werden könnte. Bestimmte Informatik-Probleme werden mit diesen Hochleistungsrechnern vermutlich schneller und effizienter gelöst werden. Auf der anderen Seite könnten dann aber auch Informationen und Daten auf Basis von klassischen Verschlüsselungsalgorithmen einfacher entschlüsselt werden. Daten, welche mit diesen kryptografischen Verfahren geschützt werden, wären dann kompromittiert.

In Zeiten von Big Data ist es besonders wichtig, die Übertragung einer enormen Datenmenge zuverlässig zu schützen, sowohl zwischen den Datenzentren als auch zwischen einzelnen Netzwerkknoten. Für die garantierte Absicherung der Information ist ein kontinuierliches Ersetzen der geheimen Schlüssel erforderlich. Bereits bei Geschwindigkeiten ab 10 G sollten die Schlüssel sehr oft ausgetauscht werden, andernfalls besteht die Gefahr, dass bei „Überlastung" eines Schlüssels genug statistische Daten gesammelt werden könnten, um die Information zu entschlüsseln.

Die Quantentechnologie hilft, diesen kontinuierlichen Austausch der Schlüssel zu bewerkstelligen. Infotecs investiert über einen Zeitraum von drei Jahren rund 4,2 Mio. Euro in die Entwicklung eines Post-Quantum-Kryptografie-Verfahrens (PQK). Das Ziel des Projektes, an dem die Forschungsabteilung von Infotecs mit internationalen wissenschaftlichen Einrichtungen eng zusammenarbeitet, ist eine marktfähige, effiziente, aber auch bezahlbare Lösung für den Aufbau eines abgesicherten Quantendatennetzes, welches gegen die Entschlüsselungsversuche von Quantenrechnern (einschließlich gegen die sogenannte aktive Erfassung) ausgelegt ist. Darüber hinaus soll das neue PQK-Verfahren die High-Speed-Übertragung bis zu 100 G über längere Strecken zwischen Datenzentren ermöglichen.

„Durch die immer performanteren Rechnersysteme steht die IT-Sicherheitsbranche vor einer äußerst schwierigen Herausforderung", kommentiert Josef Waclaw, CEO der Infotecs GmbH. „Unsere Kryptografen

arbeiten sehr intensiv bereits seit Herbst 2016 an der Entwicklung einer Post-Quantum-Kryptografie-Lösung, um unseren Kunden eine marktreife Verschlüsselungstechnologie anbieten zu können, die den geänderten zukünftigen Anforderungen an eine sichere, verschlüsselte Kommunikation gerecht wird."

Über Infotecs

Als ein führender internationaler IT-Sicherheitsanbieter sowie erfahrener Spezialist software-basierter VPN-Lösungen entwickelt Infotecs seit 1991 die Peer-to-Peer ViPNet Technologie, um mehr Sicherheit, Flexibilität und Effizienz als andere marktübliche Security-Produkte bieten zu können. Die ViPNet Security und Threat Intelligence Platform bietet komplette Sicherheit für alle Unternehmensebenen in einer einzigen kosteneffizienten Lösung. ViPNet unterstützt als einzige Technologie echte Punkt-zu-Punkt Security und gilt daher als hochsicher. Die Verschlüsselungslösung ist skalierbar, flexibel und kann einfach implementiert sowie verwaltet werden. Weiterhin kann ViPNet nahtlos in bestehende Netzwerkinfrastrukturen integriert werden, dies ermöglicht Kunden die richtige Balance zwischen hoher Sicherheit und geringer Komplexität sowie niedrigem Risiko zu finden. Mehr als 1.000.000 Endgeräte, Firmenstandorte und Server konnten bisher mithilfe von ViPNet sicher miteinander verbunden werden – unterstützt durch erfahrene Krypto-Spezialisten unseres IT-Entwicklungs- und Support-Teams sowie ein starkes Partnernetzwerk. Weitere Informationen zum Unternehmen finden Sie unter www.infotecs.de.

Kontakt

Infotecs GmbH
Anja Müller
Marketing & Kommunikation
Oberwallstr. 24
D-10117 Berlin
Tel.: +49 30 206 43 66-52
Fax: +49 30 206 43 66-66
anja.mueller@infotecs.de

Twitter: twitter.com/InfotecsDeutsch
Facebook: www.facebook.com/InfotecsGmbH
Xing: www.xing.com/companies/infotecsinternetsecuritysoftwaregmbh
Google+: plus.google.com/+InfotecsDe/
LinkedIn: www.linkedin.com/company/infotecs-internet-security-software-gmbh