SpecialInterest

» Schutz vor Cyber-Kriminellen der Zukunft «

Quantenresistente Ethernet-Verschlüsselung als „Plug&Play“

Welche Konsequenzen hat es, wenn ein Quantencomputer von Google eine mathematische Aufgabe in Minuten löst, für die ein halbleiterbasierter Supercomputer 10.000 Jahre benötigt? Zunächst einmal weckt es Zweifel am Ergebnis. So behauptet IBM, die mathematische Aufgabenstellung sei mit konventionellen Mitteln in „nur“ 2,5 Tagen zu lösen gewesen. Dennoch beweist das Experiment, das Quantencomputer ein immenses Potenzial bergen.

Netzwerksicherheit: eine Frage der Mathematik

Wer heute sein Ethernet-Connect verschlüsselt, vertraut ebenfalls auf eine mathematische Aufgabenstellung, deren Lösung unpraktikabel viel Rechenleistung verschlingt. Dabei ist es nur eine Frage der Zeit, bis Quantencomputer in der Lage sind, auch solche Aufgaben zu lösen und bewährte Verschlüsselungsverfahren zu knacken.

Während nämlich traditionelle Computer auf Bits basieren, die entweder einen Wert von 0 (Strom aus) oder 1 (Strom an) annehmen können und damit definierbare und reproduzierbare Zustände liefern, gelten in der Quantenwelt – aufgrund der Superposition sowie Quantenverschränkung – andere Regeln.

Und selbst Qubits, also die kleinste Recheneinheit eines Quantencomputers, sind mit unserem Alltags-Determinismus kaum zu fassen: Sie können theoretisch mehrere Zustände gleichzeitig einnehmen und eröffnen neue Möglichkeiten für die Lösung mathematischer Probleme.

Asymmetrische versus symmetrischer Verfahren

Um zu verstehen, wo Quantencomputer ihren Vorteil ausspielen können, muss man die Verschlüsselungskonzepte betrachten:

» Asymmetrische Kryptosysteme basieren meist auf der Kalkulation diskreter Logarithmen und der Primfaktorzerlegung. Diese könnten zukünftig durch den Shor-Algorithmus gelöst werden und bieten damit eine gewisse Angriffsfläche für Quantencomputer.

» Bei symmetrischen Verschlüsselungsverfahren wie AES verfügen beide Teilnehmer über denselben Key. Mittels Grover-Algorithmus ließe sich die effektive Schlüssellänge im besten Fall von 256 Bit auf 128 Bit reduzieren. Daher bietet AES mit einem 256 Bit Key aus der Sicht der quantenresistenten Kryptographie ausreichend Schutz für die kommenden Jahrzehnte.

Schutz für Ihr Ethernet-Connect

Um Ihre Ethernet-Verbindung vor den Bedrohungen von heute und vor leistungsfähigen, universellen Quantencomputern von morgen zu schützen, benötigt es einer quantenresistenten Verschlüsselung (Post-Quanten-Kryptographie). Als Partner des führenden Anbieters für quantenresistente Verschlüsselungen in Deutschland erhalten Sie von der Pan Dacom Direkt eine Kryptographie-Lösung, die dank einer Kombination aus den besten asymmetrischen und symmetrischen Verschlüsselungsverfahren Ihre Netzwerke effektiv vor den Cyber-Kriminellen der Zukunft schützt.

Ob Sie nun eine verschlüsselte Punkt-zu-Punkt- oder zu-Multipunkt-Verbindung planen oder nachrüsten wollen: Wir bieten Ihnen eine einfach zu installierende Lösung an, die Ihr System effektiv auf Layer 2/3 schützt, BSI-konform ist und – anders als IPSec – vollen nativen Durchsatz für 10/40/100G erlaubt.

Dank des starken Integritäts- und Replayschutzes bietet das System auch gegen aktive Angriffe mittels AES-GCM und L2Sec. Einmal installiert, benötigen die Geräte nahezu keinen Wartungsaufwand. Abhängigkeiten von anderen externen Geräten oder Servern entfallen, sodass kein Fremdzugriff aus dem Netz möglich ist. Auf Wunsch können wir Ihnen die Geräte auch vorkonfiguriert anliefern.

Quantenresistenz kostet nicht die Welt: Wir bieten Verschlüsselungslösungen passend zur Ihrem Datendurchsatz und Ihrer Netzwerkinfrastruktur.

» Auf einen Blick

Die Herausforderung:

» Mehrere Millionen Angriffsversuche pro Jahr auf deutsche Netzwerke

» Quantencomputer, die in naher Zukunft bewährte Verschlüsselungsverfahren aushebeln werden

Die Lösung:

» Quantenresistente Kryptographie als einfach zu installierende Lösung für Managed-Service-Verbindungen/Ethernet-Connect

Die Vorteile:

» **Starker Integritäts- und Replayschutz gegen aktive Angriffe**

» **Uneingeschränkt für Managed-Service-Verbindungen**

» **Autonomer Langzeitbetrieb, mit 4 bis 6 Jahren BSI-Zulassung**

» **Verwendung beliebiger L1/L2/L3 WAN Technologien**

» **Einfache und sichere IPv6 Migration**

» **Einfach zu installieren und konfigurieren: Plug&Play-Verschlüsselung**

» **Hoher Datendurchsatz**

» **Lange Nutzungsdauer durch FPGA-Technologie**

» **„Made in Germany“, unabhängig von Wirtschaft und Politik**

20201221