dataport

Stefan **Schumacher:**

Post-Quanten-Kryptographie: die Zukunft der Informationssicherheit



Di., 30. Sep. 2025, 15:30–15:45 Uhr
Speakers Corner am Dataport Stand

SMART COUNTRY CONVENTION

Kryptographie

- Kryptographie basiert auf mathematischen Einwegfunktionen
- leicht in eine Richtung zu lösen, aber sehr schwer umkehrbar
- z.B. zerlegen einer großen Zahl in ihre Primfaktoren
- $344\,707 = 11 * 31337$
- die große Zahl hat in der Praxis ca. 1 300 Stellen

Quantencomputer

- können mehrere Zustände parallel annehmen
- und sehr effizient z.B. Primfaktoren berechnen
- damit traditionelle Kryptographie brechen

Quantencomputer

- können mehrere Zustände parallel annehmen
- und sehr effizient z.B. Primfaktoren berechnen
- damit traditionelle Kryptographie brechen
- wir brauchen quantensichere Kryptographie!
- Post-Quanten-Kryptographie

Neue Standards

- US NIST FIPS 203 Module-Lattice-Based Key-Encapsulation Mechanism
- US NIST FIPS 204 Module-Lattice-Based Digital Signature Standard
- US NIST FIPS 205 Stateless Hash-Based Digital Signature Standard
- derzeit Hybridverfahren aus ECC und PQC empfohlen
- durch OpenSSL 3.5 und BouncyCastle unterstützt

Was ist zu tun?

- Krypto-Kataster: Wo findet Verschlüsselung statt?
  Datenflussdiagramme, Schnittstellendefinitionen
  TLS, Backups, Datenbanken, Firmware ...
- Jetzt: Hybrid – später Ersetzen: Prä- und Post-QC kombinieren (z.b. tunneln oder überschlüsseln)
- Kryptoagilität: Algorithmen und Cipher-Suiten austauschbar einbinden
- Data at Rest und Data in Motion: Datenbanken, Dateisysteme, Storage, Backups, VPNs, SSH, QUIC, WebRTC, Zertifikate, HSM
- Hardwaretoken: FIDO2 Passkeys, Yubikey, Nitrokey, Token2 ...
- Entwicklung: Frameworks und Bibliotheken beobachten, Interoperabilität überwachen, Schlüssel rotierbar halten
- Maßnahmenplan: Compliance erfordert Migrationspläne mit Umsetzungsplan *jetzt*!



- stefan.schumacher2@dataport.de
- cryptomancer.de/kryptokalypse
- cryptomancer.de/pqcbenchmark