genua.

Postquantenmigration

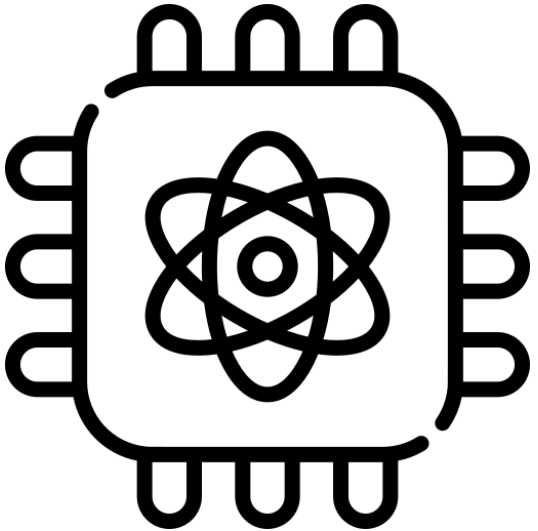
Brauchen wir das und wenn ja wie?

Daniel Herzinger, genua gmbh
PQC-Kryptograph

16.09.2025, Congress Park Hanau

Der Quantencomputer und die Kryptographie

- Shor's Algorithmus
- Bricht asymmetrische Verschlüsselung
- Benötigt leistungsstarken Quantencomputer
- „Store now, decrypt later“ jetzt schon relevant



Wie viel Zeit haben wir noch?

„[…] Damit ist es wahrscheinlich, dass selbst ohne Disruptionen ein krypotanalytisch relevanter Quantencomputer in höchstens 16 Jahren realisierbar ist.

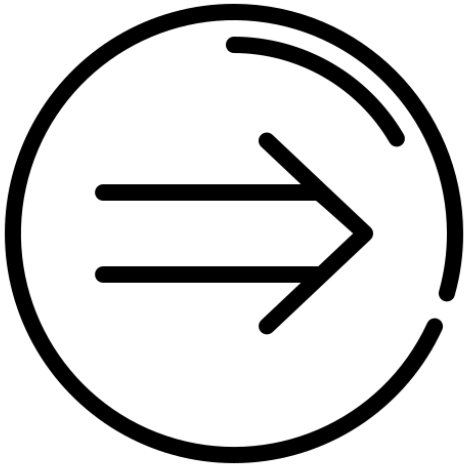
Zudem gibt es inzwischen eine Fülle neuer Entwicklungen bei der Fehlerkorrektur und -mitigation sowie der Hardware, die dies deutlich auf knapp zehn Jahre beschleunigen könnten, aber noch nicht durchgängig verifiziert sind.“

– BSI, Entwicklungsstand Quantencomputer

Regulatorik schafft Fakten

- Bei regulierten Organisationen (EU):
  - „Store now, decrypt later“ spätestens bis 2030
  - PKIs mit langen Laufzeiten bis 2030: Konzept
  - Für volle Migration noch keine Deadline
- High Assurance Cryptographic Equipment (Australien):
  - Bis 2030 Austausch von:
    - RSA
    - ECDSA
    - ECDH
    - SHA-256
- Weltweiter Tenor geht in ähnliche Richtung

Implikationen



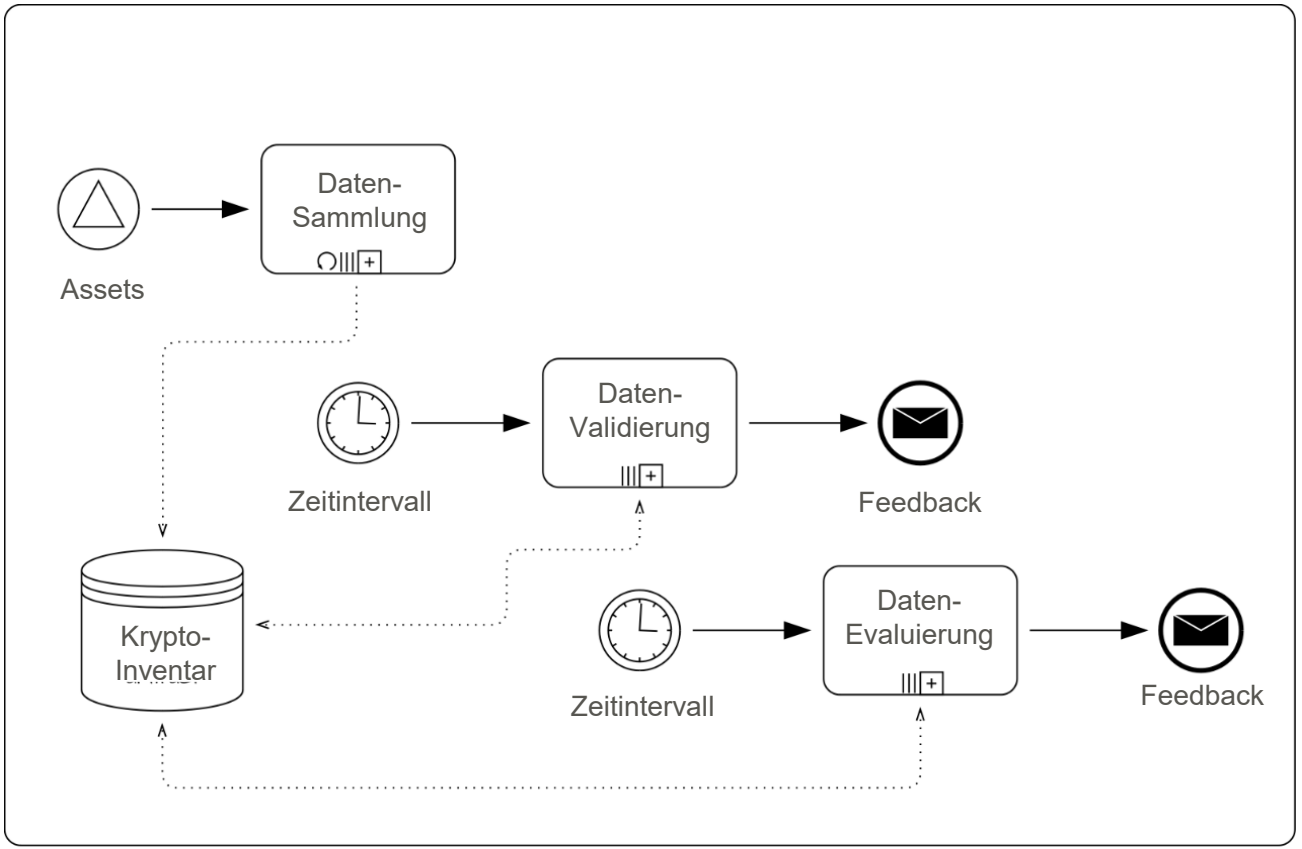
- Postquantenmigration im regulierten Umfeld unausweichlich und dringend
- Tatsächliche Sicherheit der PQC-Verfahren noch nicht eindeutig
- Keine einheitliche Meinung zu hybriden Verfahren
- Viele Annahmen für Entscheidungen

⇒ (Krypto-)Agilität ist der Schlüssel

Kryptoagilität – Theorie

- Kryptoagilität ≈ Effiziente Migrierbarkeit von kryptographischen Systemen im gegebenen Kontext bei Aufrechterhaltung der Geschäftsprozesse
- Migrieren eines Systems
  - Tauschen
  - Ändern (Migrieren eines Subsystems)
  - Kapseln
- Kapseln ≠ Migration ?
- Interoperabilität als Enabler

Kryptoagilität – GAIN – 1. Gather



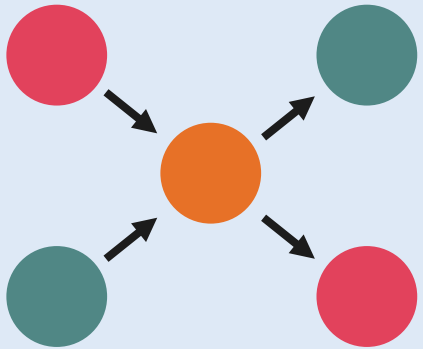
Datensammlungsansätze

- Fragebögen
- Abhängigkeitsanalyse
- Dokumentation
- Netzwerkanalyse
- Konfigurationsanalyse
- Statische Code-Analyse

...

Kryptoagilität – GAIN – 2. Assess

1. Priorisierung

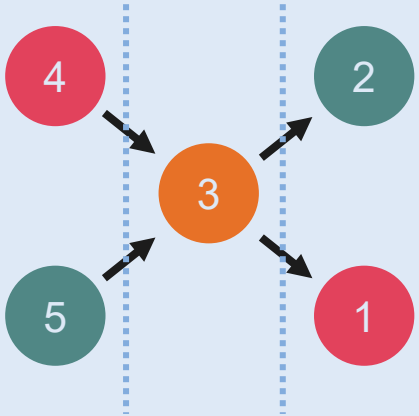


: Hohe Priorität

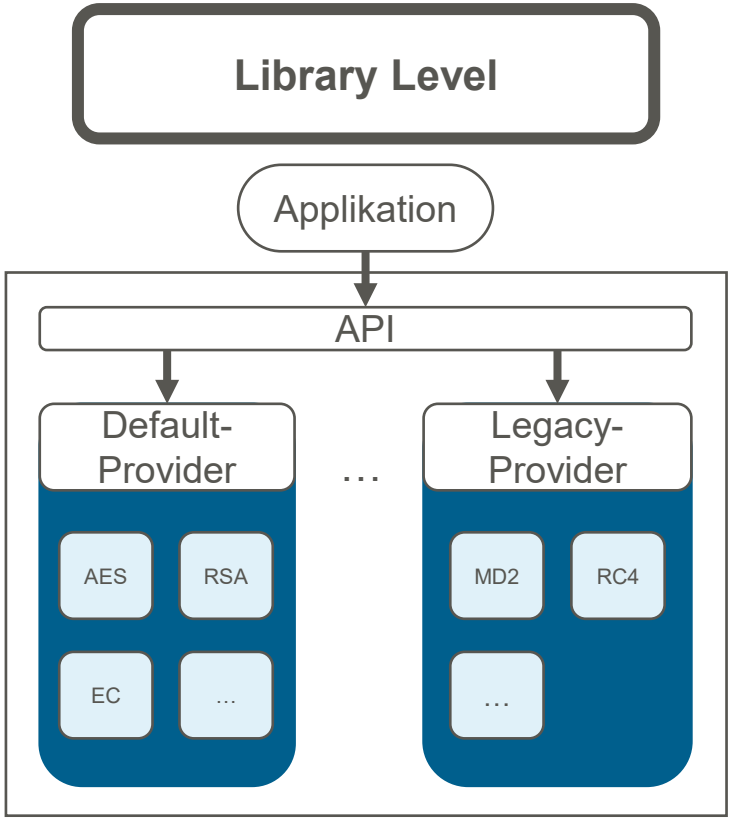
: Mittlere Priorität

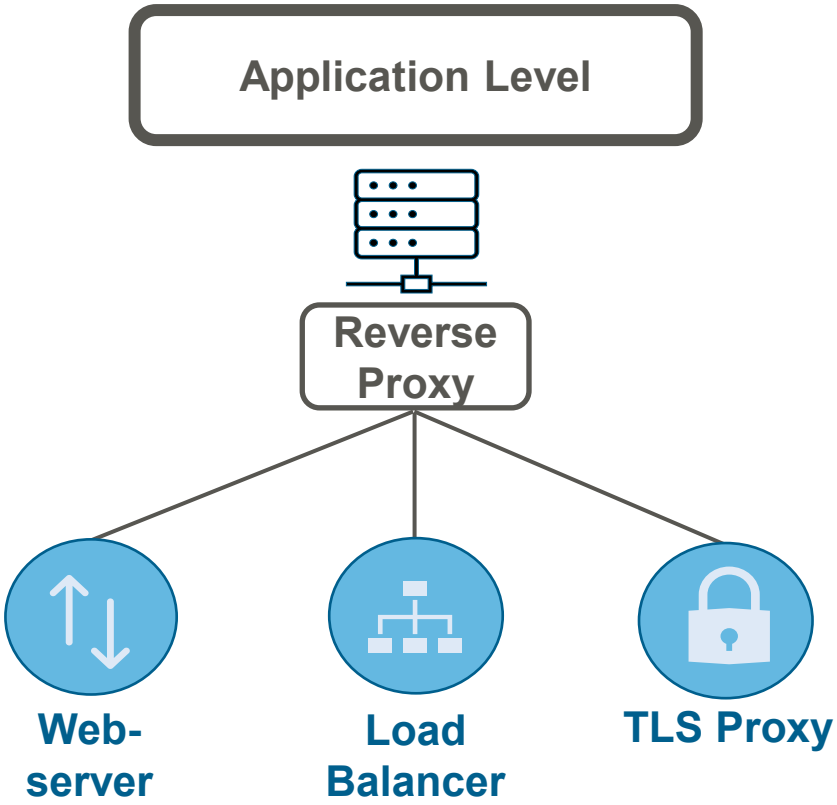
: Geringe Priorität

2. Clustering & Schätzen



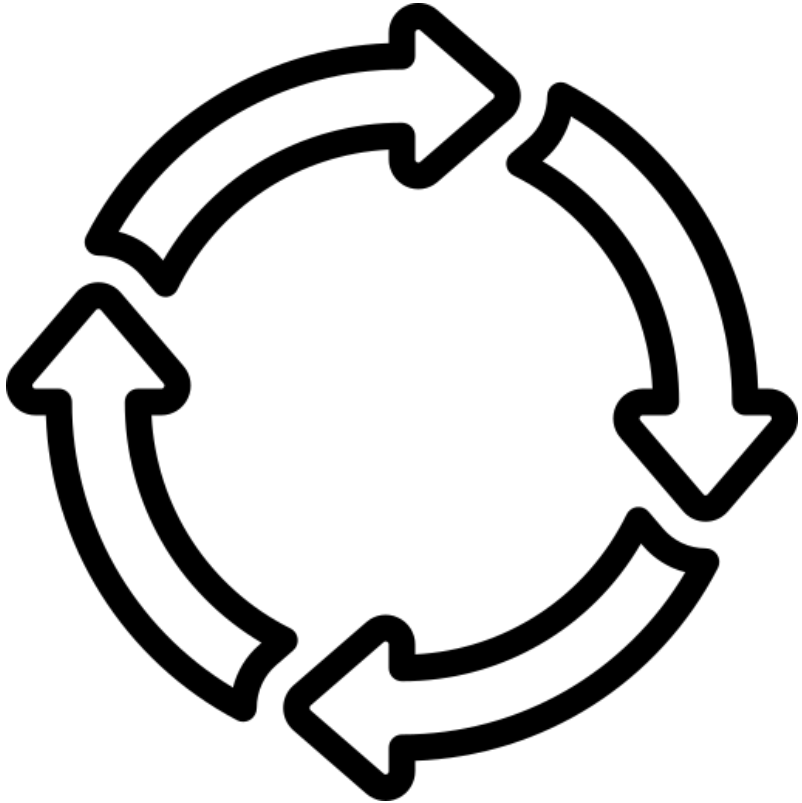
Kryptoagilität – GAIN – 3. Implement





Kryptoagilität – GAIN – 4. Nurture

- Prozess ist nie 100% abgeschlossen
- **Ziel:** Gelebter Prozess inkl. technischer Umsetzung für Management von Kryptographie und Kryptoagilität



Tooling für Kryptoagilität – Status Quo

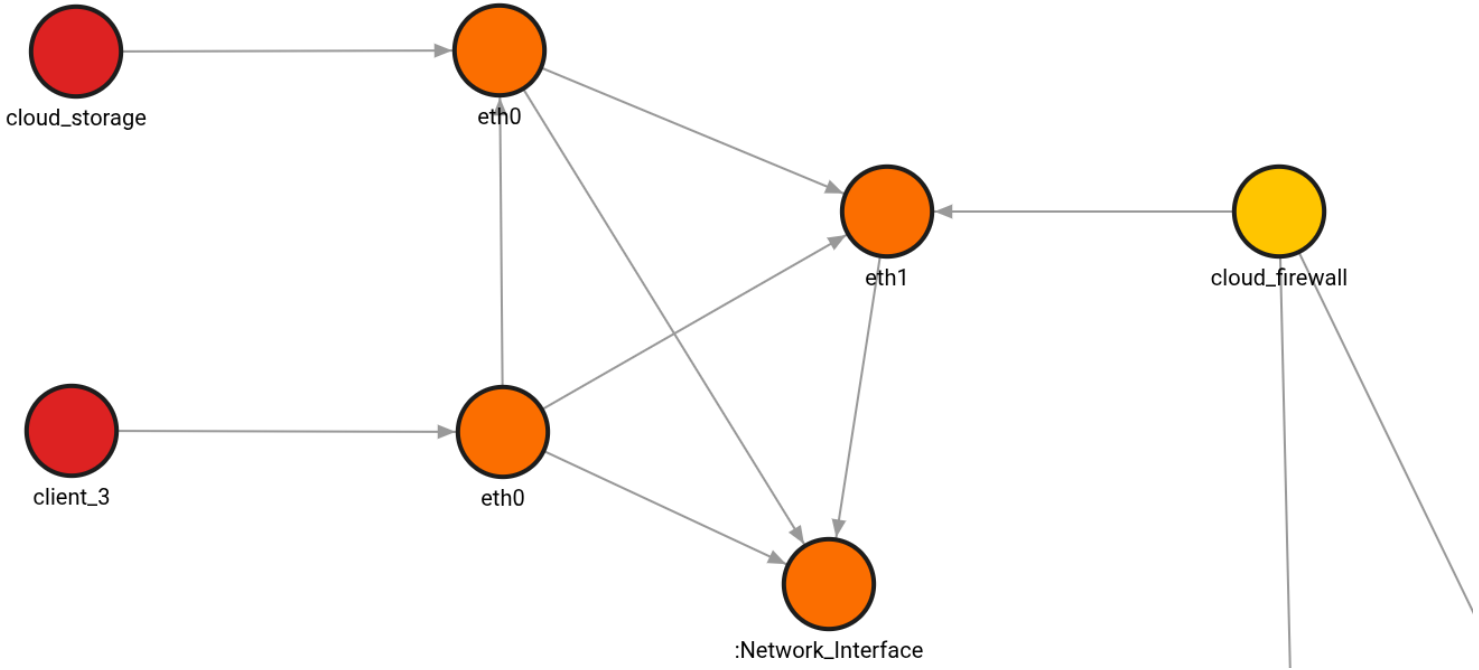
- Diverse Ansätze für
  - Datensammlung
  - Inventarisierung
  - Datenmodellierung
- CBOMs vielversprechendes Konzept
- Woher kommt der Inhalt der CBOMs?
- Aufbereitung der CBOMs?
- Zusätzlich relevanter Kontext?

  → Wenig Konzepte für Sammlung und Kontextualisierung

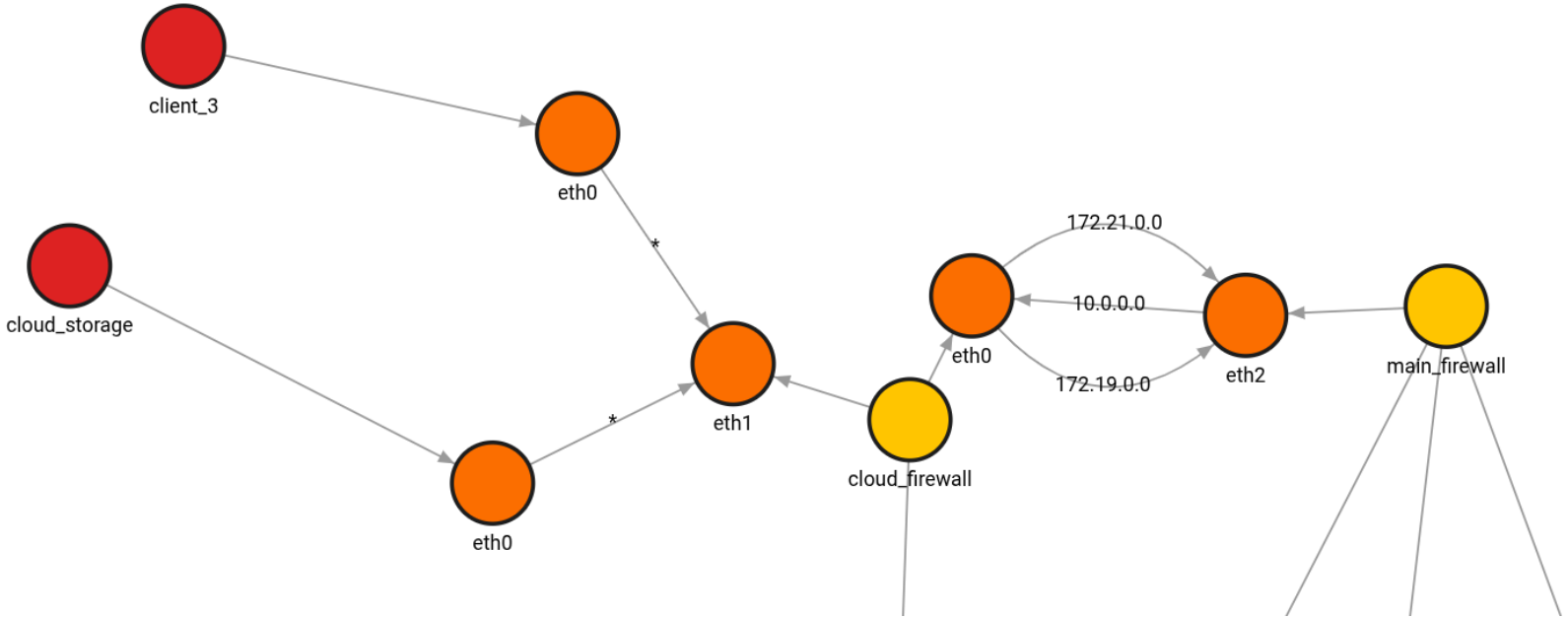
Tooling für Krypto-Agilität – Unser Ansatz

- Fokus auf Kryptoinventar + Netzwerkkontext
- Layer 2 & 3 Topologie durch:
  - Geräteinspektion: Welches System hat welche Interfaces
  - Geräteinspektion: Routing Tables
  - ARP Sniffing
- Layer 4 Topologie (Verbindungen) durch
  - Deep Packet Inspection
  - Inklusive Kryptoparameter
- Kryptoinformationen durch CBOMs

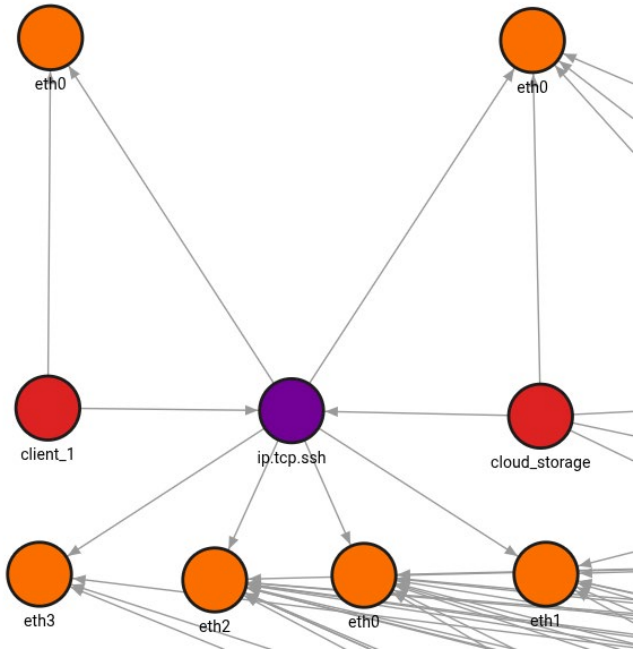
Tooling für Kryptoagilität – Demonstrator – Layer 2



Tooling für Kryptoagilität – Demonstrator – Routing



Tooling für Kryptoagilität – Demonstrator – Verbindungen




```
dest_ip: "10.20.0.2"
protocol_path: "ip.tcp.ssh"
source_ip: "172.19.0.2"
tsp_alg_kex:
"'sntrup761x25519-
sha512@openssh.com,curve2551
9-sha256,curve25519-
sha256@libssh.org,ecdh-sha2-
nistp256,ecdh-sha2-
nistp384,ecdh-sha2-
nistp521,diffie-hellman-
group-exchange-
sha256,diffie-hellman-
group16-sha512,diffie-
hellman-group18-
sha512,diffie-hellman-
group14-sha256,ext-info-
c,kex-strict-c-
v00@openssh.com';'sntrup761x
25519-
sha512@openssh.com,curve2551
9-sha256,curve25519-
sha256@libssh.org,ecdh-sha2-
nistp256,ecdh-sha2-
nistp384,ecdh-sha2-
nistp521,diffie-hellman-
group-exchange-
sha256,diffie-hellman-
group16-sha512,diffie-
hellman-group18-
sha512,diffie-hellman-
group14-sha256,ext-info-
s,kex-strict-s-
v00@openssh.com'"
```

Fazit

- PQC-Migration rollt voll auf uns zu
- Kryptoagilität von zentraler Bedeutung
- Zirkulärer Prozess
  - Erkennen von Kryptographie
  - Erkennen von Abhängigkeiten
  - Priorisieren von Kryptographie
  - Reduzieren von Abhängigkeiten
- Tooling kommt
- CBOMs entwickeln sich zu de-facto Standard

Controlware
Security Day

Danke für Ihre Aufmerksamkeit.
Wir freuen uns über Ihr Feedback!

Bitte geben Sie den ausgefüllten Bogen am Empfang ab und erhalten Sie als Dankeschön ein kleines Präsent.