

Post-Quanten-Kryptografie

Von der regulatorischen Anforderung zur kryptografischen Resilienz

Know-how to go | 10. Juni 2026

Marvin Sprey

Agenda

A long cable-stayed bridge spans a body of water under a dramatic, cloudy sky at sunset or sunrise. The bridge features a prominent A-frame pylon and numerous stay cables. The water is calm, reflecting the bridge and the sky. The overall mood is serene and majestic.

1. Einordnung

2. Bedrohungslage

3. Herausforderung

4. Der Weg

Marvin Sprey Consultant



- Beratung und Begleitung von Unternehmen bei der Einführung und Verbesserung ihrer Informationssicherheitsmanagementsysteme
- Kryptografie im regulatorischen Kontext: Sicherheitskonzepte, Richtlinien und Prüfung kryptografischer Anforderungen
- Entwicklung eines strukturierten Vorgehens zur Begleitung von Unternehmen auf dem Weg zur Krypto-Agilität
- Kryptografische Bestandsaufnahme, Risikobewertung und Migrationsplanung im Kontext Post-Quanten-Kryptografie
- Sensibilisierung und Wissenstransfer durch Fachvorträge, Workshops und gezielte Awareness-Maßnahmen

1. Einordnung



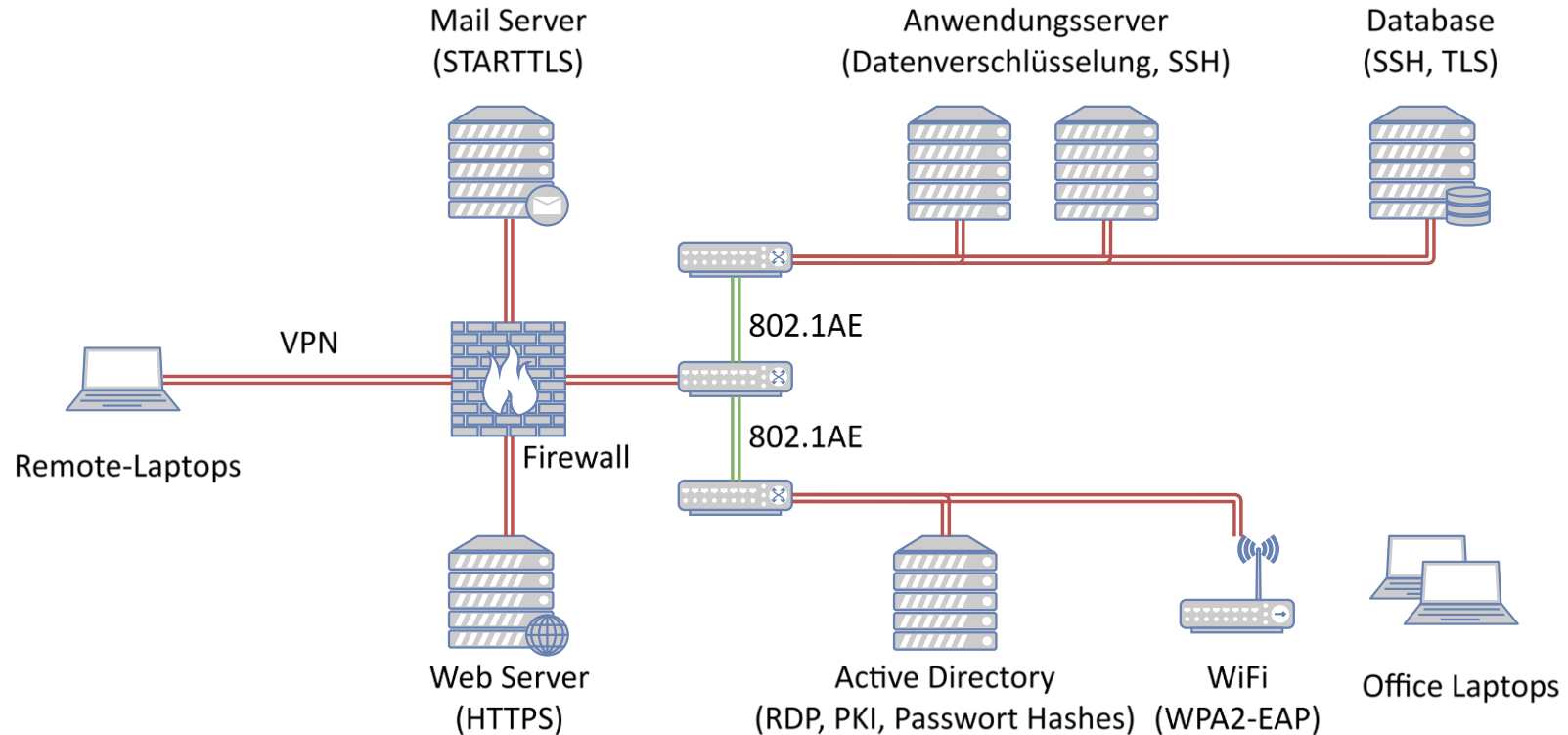
Kryptografie nach dem Stand der Technik

Die eine Forderung, die alle Gesetze gemeinsam haben



Wo steckt überall Kryptografie?

Kryptografie in einer typischen Unternehmensinfrastruktur



2. Bedrohungslage



Warum das zum Problem wird

Quantencomputer, Shors Algorithmus und Post-Quanten-Kryptografie

Das Problem



Heutige (Public-key-)Algorithmen:

RSA - Faktorisierung von Primzahlen

DH - Diskreter Logarithmus

Shors Algorithmus

→ In Polynomialzeit lösbar

Die Antwort



Post-Quanten-Kryptografie:

ML-KEM, FrodoKEM, Classic McEliece

ML-DSA, SLH-DSA

Andere mathematische Grundlagen
(Gitter, Hashes)

→ Auch für kryptografisch relevante
Quantencomputer (realistisch) unlösbar

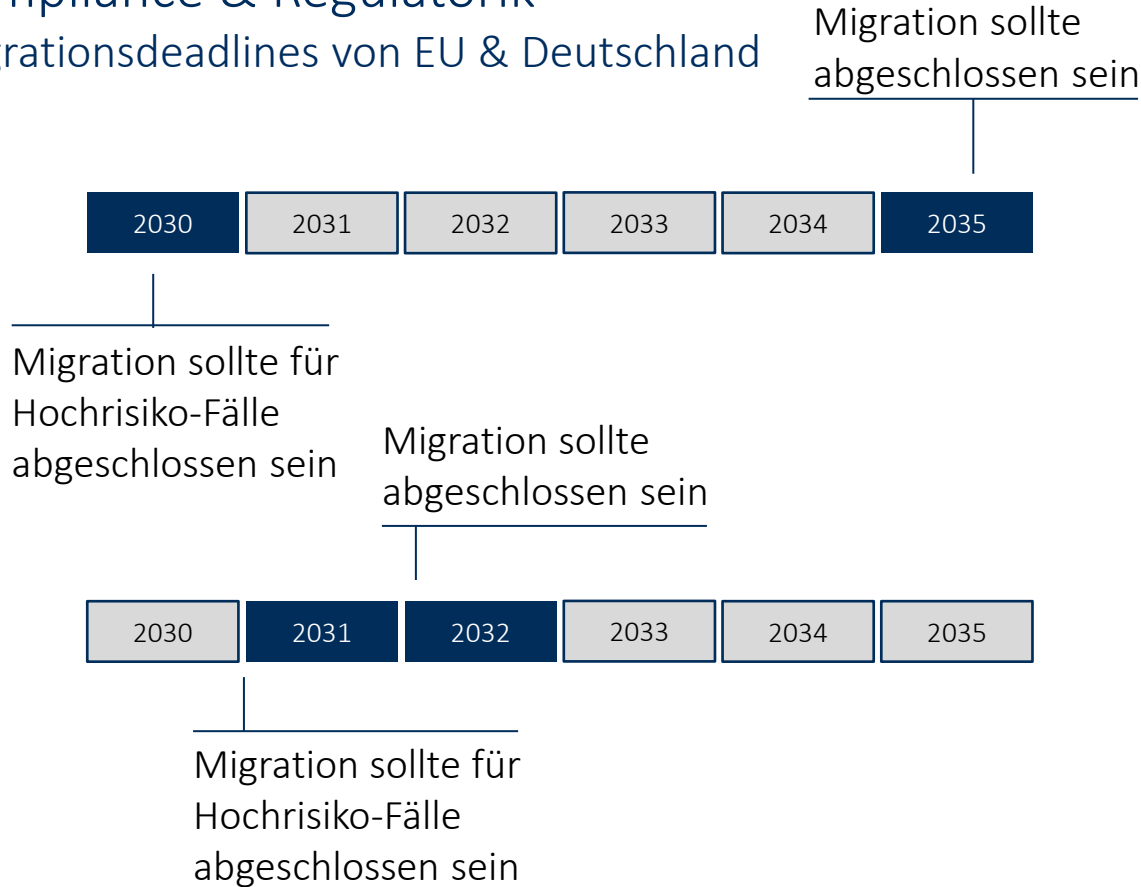
Harvest Now, Decrypt Later

Warum die Quantenbedrohung schon vor dem Quantencomputer real ist



Compliance & Regulatorik

Migrationsdeadlines von EU & Deutschland

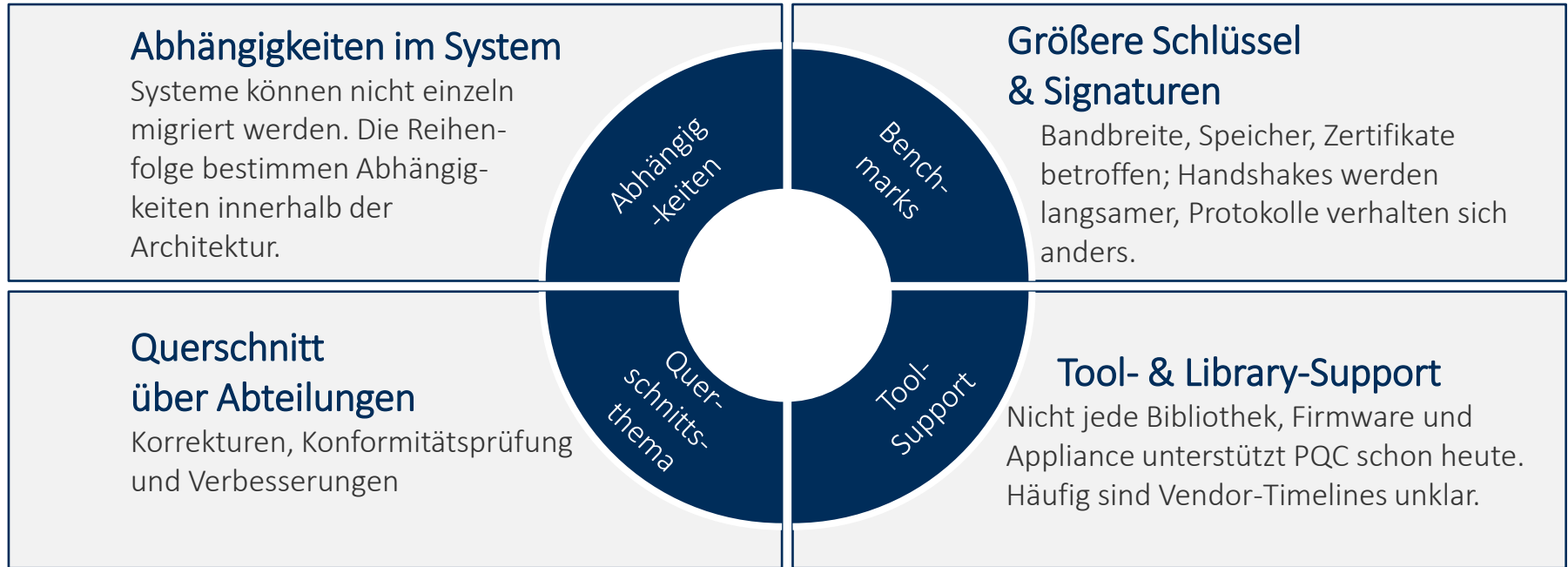


3. Herausforderung

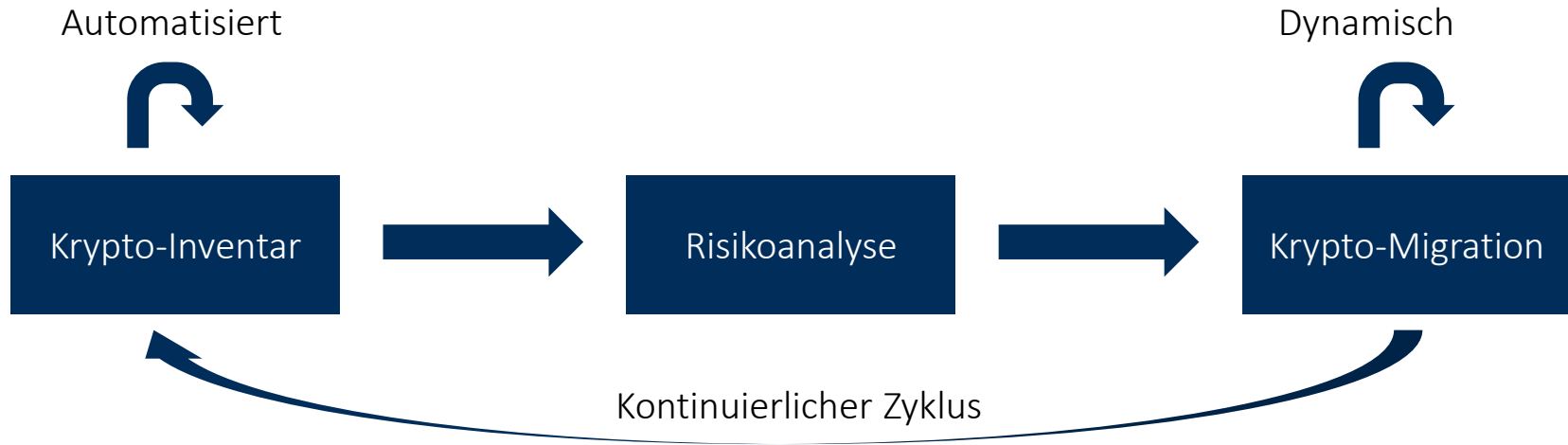


Warum die Migration kein einfaches Update ist

Ein Querschnittsthema mit technischen und organisatorischen Hürden



Krypto-Agilität als Zielbild



Fraunhofer:

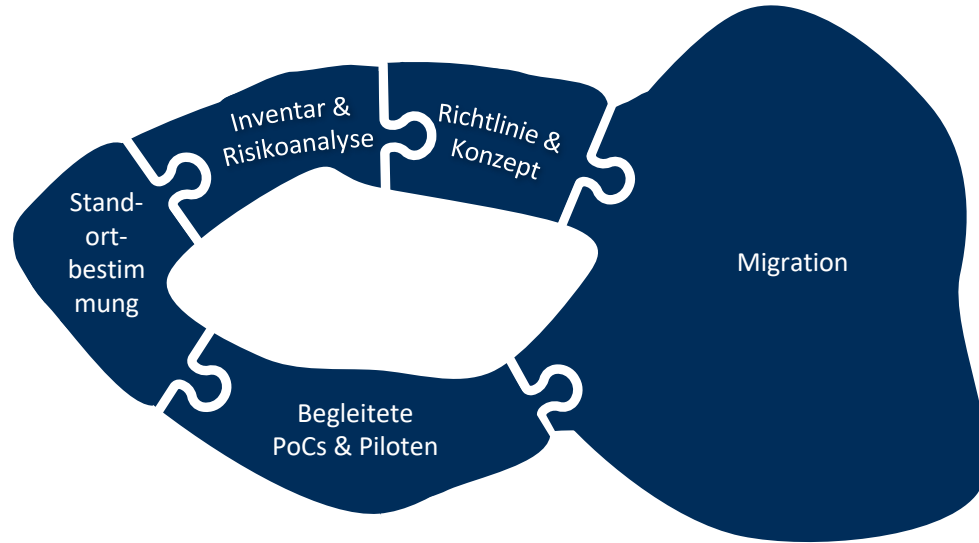
„Krypto-Agilität bezeichnet die Fähigkeit eines Systems oder einer Organisation, die genutzte Kryptografie flexibel anzupassen und so schnell auf neu entdeckte Schwachstellen zu reagieren.“¹

4. Der Weg



Der Weg zur Krypto-Agilität

Ein strukturierter Pfad zur Krypto-Agilität; empfohlen von u. a. BSI, TNO & NIST



Für wen ist das relevant?



Kryptografische Standortbestimmung

Kryptografische Reife bewerten und Geschäftsauswirkungen verstehen

Stufe	Name
1	Ad hoc
2	Sensibilisiert
3	Strukturiert
4	Operativ
5	Optimierend

Was passiert hier?



Sichtung der Architektur & eingesetzter Kryptografie



Regulatorische Anforderungen zuordnen



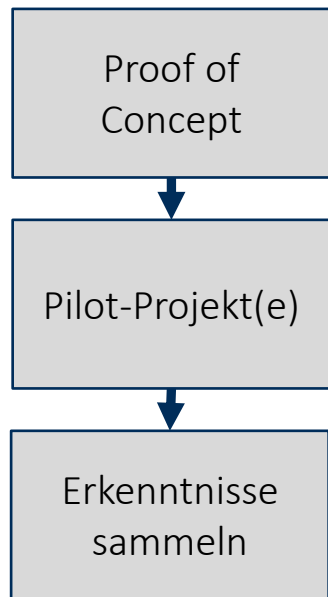
Business-Impact-Analyse: Welche Daten müssen wie lange geheim bleiben?

→ Priorisierung & Reifegradbestimmung

Pilotprojekte & Proof of Concepts

Erfahrung sammeln, bevor es in die Breite geht

Bevor eine unternehmensweite Migration beginnt, sollten gezielte Proof-of-Concepts und Pilotprojekte die praktische Machbarkeit und mögliche Stolpersteine aufzeigen. Diese Phase sollte parallel zur Inventarisierung und Governance-Anpassungen laufen.



Bereich
TLS
PKI
VPN
E-Mail

Ziele der Pilotphase
✓ Wissensaufbau im Unternehmen
✓ Frühzeitiges Erkennen von Problemen
✓ Interoperabilitätstests
✓ Performance-Validierung

Kryptografie inventarisieren und Risiken bewerten

Man kann nicht schützen, was man nicht kennt

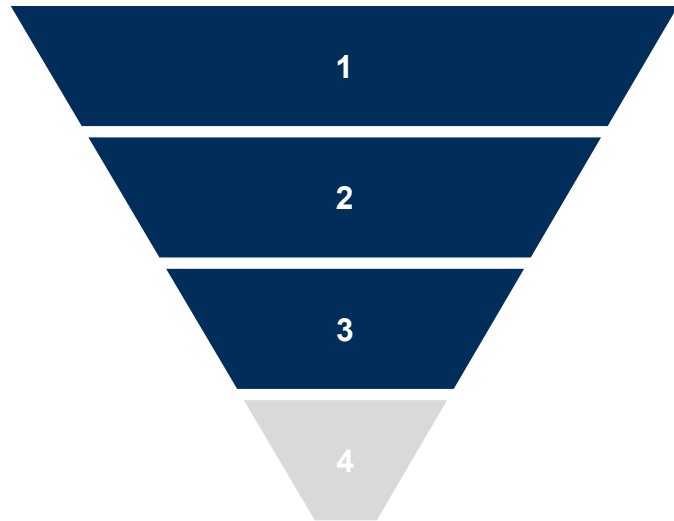


 Operative Kryptografie	 Kryptografie in Software	 Kryptografie in Netzwerken	 Kryptografie in Hardware
PKI, Schlüssel, Konfigurationen, Data-at-Rest, OT, ...	Libraries, Hardcodierte Assets, ...	Protokolle, Data-in-Transit, VPNs, ...	Verwaltete Schlüssel, HSMs

	Kategorie	Beschreibung
	Kein akutes Risiko	Kryptografie entspricht aktuellen Standards
	Quanten-Risiko	Migration notwendig, aber Zeitfenster vorhanden
	Akutes Risiko	Veraltete Verfahren oder zeitkritische Daten

Governance

Kryptografie durch Richtlinien, Konzepte und Prozesse verankern



Von Anforderungen
Zu Maßnahmen

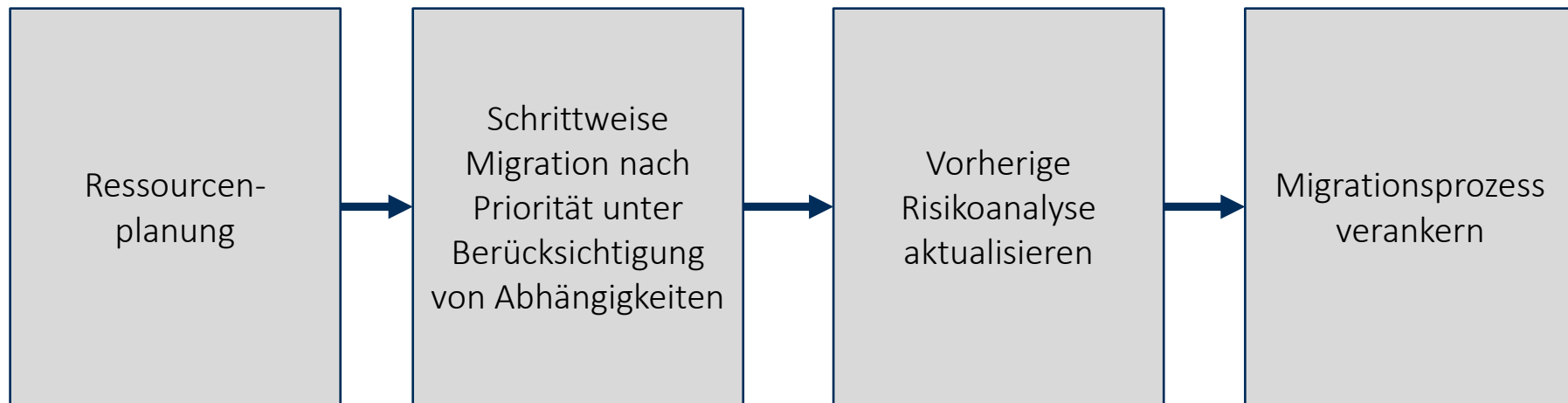
- 1 Regulatorischen Rahmen & Erkenntnisse konsolidieren
- 2 Kryptografische Richtlinie & Krypto-Konzept erstellen, betroffene Dokumente anpassen
- 3 Betroffene Prozesse anpassen
- 4 Governance-Strukturen verankern

Migrieren: priorisiert und hybrid

Vom Piloten in den Regelbetrieb

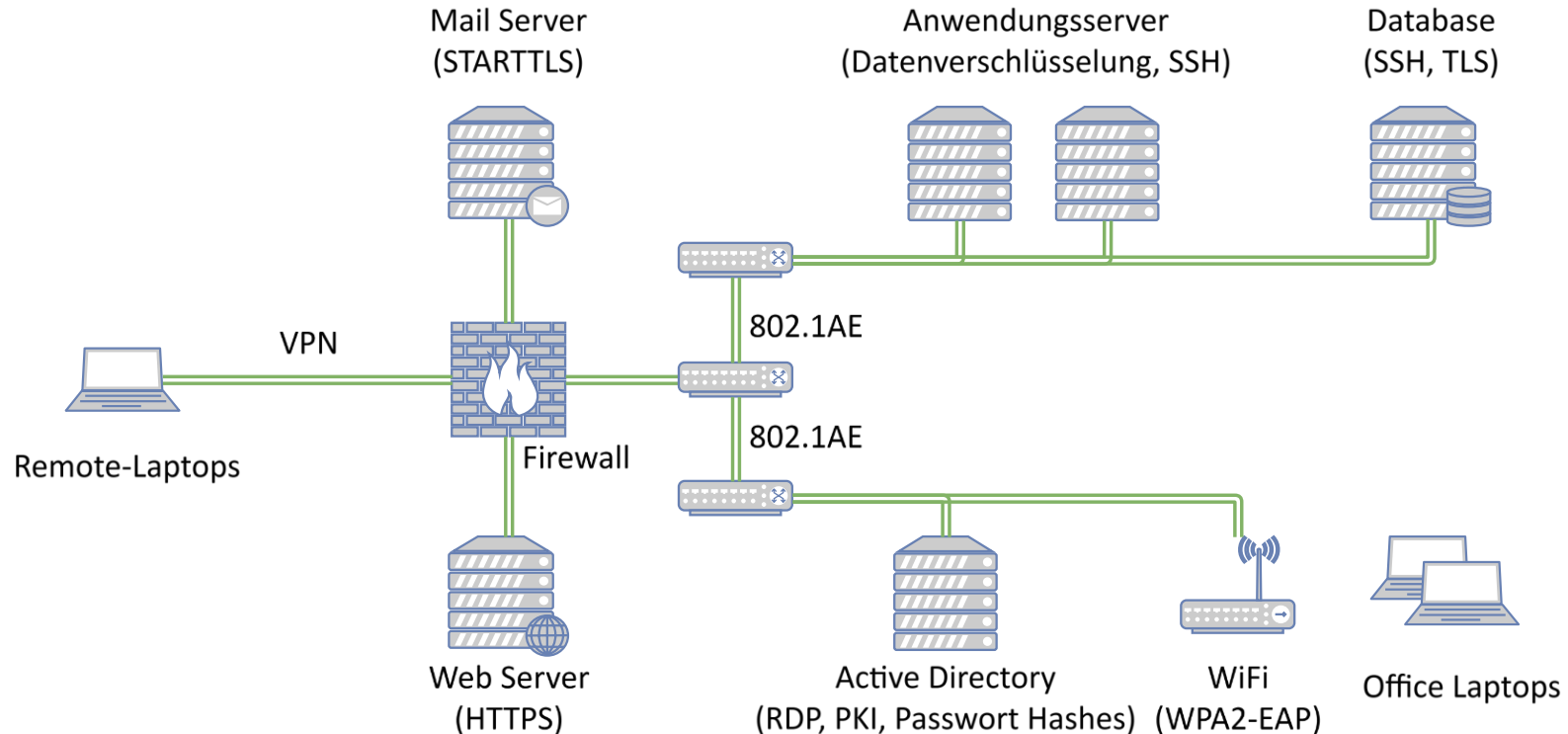


PQC ist komplex. Bevor die Migration beginnt, benötigen Entwickler, Administratoren und System-Architekten ein fundiertes Verständnis für krypto-agile Prinzipien, die einzusetzenden Verfahren und hybride Implementierungen.



Kryptografie ist kein Feature – sie ist das Fundament

Warum Krypto-Agilität keine Option, sondern eine Notwendigkeit ist



Kontakt

Marvin Sprey
Consultant

