
FUTURE CONNECTIONS
CIRCLE
Powered by:
digicert

Unser Team vor Ort

Leonhard Roschlau

Anja Breyer

OPENING

Ausblick auf einen interaktiven Nachmittag

Leonhard Roschlau

Business Unit Manager
LSZ Future Connections

Christian Müller

Regional Vice President
DigiCert

FUTURE CONNECTIONS

CIRCLE

Powered by:

digicert

Future Connections Circle

VORSTELLUNGSRUNDE & KENNENLERNEN

DISKUSSIONSIMPULS

Krypto-agility for the win! Wie Entscheider:innen Komplexitätstreibern der Cyber- und Informationssicherheit wie DORA, NIS2 oder PQC erfolgreich begegnen

Christian Müller

Regional Vice President
DigiCert

Ralph Jung

Senior Projektmanager & Consultant
HST GmbH Technische Entwicklungen

FUTURE CONNECTIONS

CIRCLE

Powered by:

digicert

digicert®

DigiCert
Lösung & Zukunftsicherheit

DigiCert Firmenimpuls
Christian.mueller@digicert.com

Einschätzung führender Analysten

PKI is a fundamental building block for **establishing digital trust.**

As certificates continue to gain importance in securing organizations, **effective management of digital trust** becomes imperative.

Gartner®

Bedarfstreiber der Krypto-Agilität der PKI

Exponentiell ansteigende Maschinenidentitäten

Verkürzte Zerfitikatslaufzeiten

Post-Quantum Kryptographie

Hauptgründe der exponentiellen Komplexitätssteigerung (x8/5Y.)

Verkürzung der Lebensdauer
von Zertifikaten und Validierungen
(398 auf - 47 Tage / 8x mehr Aufwand)
-> erhöhte Risiken

1

Gesetzliche Vorschriften/
Compliance / Regulatorik / Industriestandards
(NIS2, DORA ,EU Cyber Resilience Act,
Eidas 2.++)

2

Vertrauenswürdigkeit von AI
Content (Videos/Fotos) &
AI Agents/Chatbots
IoT Anwendungen
Verwebung von IT / OT

3

Quantencomputing &
Einfluss auf Kryptographie
“Post-quantum Cryptography” (PQC)

4

Es bedarf einer nachhaltigen, modularen Trust- und Prozesslogik, die alle digitalen Identitäten hoch-automatisiert, standardisiert und ganzheitlich, zukunftsicher und in „Compliance“ by Design abdeckt - Insellösungen enden im Disaster -

Cypto-Agilitäts-Modell – „der fast track“ zur Pos. #4 ist von zentraler Bedeutung

80% der Unternehmen sind hier

1 By Incident

- Manuelle Prozesse
- Sicherheitsrisiken
- Ausfälle

2 Reactive

- Transparenz
- Alerting & Reporting
- Regelmäßige Audits

3 Proactive

- Automatisierte CSR
- Richtlinienkonformität
- Self-service Portale
- Policies & Governance

4 Automation

- Volle Automatisierung
- Rollenbasierte Zugriffe
- Nahtlose Integration
- Kaum Resourcenbindung

5 Crypto-Agile

- Schnelle und strukturierte Antworten bei Incidents
- PQC Ready
- Ready für kürzere Laufzeiten
- Endpoint Ready

20% sind hier

Crypto-Agiltät

Transparenz & Automatisierung

Führend in Standardgremien des Zertifikatsmanagements

Driving Global Standards

CA/BROWSER FORUM

NIST

CLOUD SIGNATURE CONSORTIUM

IETF

CableLabs

ETSI

ICANN

C2PA

ACME

X9

CI+

matter

SCITT

Operationale Exzellenz Daten

25+
Annual audits

99.99%
Uptime SLA

3,100+
Annual key ceremony

2,600+
Global public and private roots

24/7/365
World-class support

80+
NPS

Unser Auftrag als Weltmarktführer: Sharing Excellence

90%
Fortune 500 companies

180
Countries served

65%
Ecommerce secured

8B+
Machine identities

80+
Net promoter score

Technology	Finance & Insurance	Manufacturing & Energy	Healthcare	Automotive	Consumer
IBM	Deutsche Bank	BOSCH	B|BRAUN		BOSCH Smart Home Technik fürs Leben
salesforce	Sparkasse	ABB	Cigna.		SAMSUNG
SAP	Allianz	e·on	Scripps	BMW	eve. by ABB
SIEMENS	UBS Financial Services Group	Hitachi Energy	labcorp	TESLA	UNDER ARMOUR

digicert®

Grundlagen der Crypto-Agilität

Transparenz, Inventarisierung und operative Resilienz

Ralph Jung HST GmbH
ralph.jung@hsti.de

Treiber - Compliance und Vorbereitung auf PQC

Aktuelle Regulatorien

- ISO 27001/27002
- NIS2
- DORA / BAIT / KAIT / VAIT
- KRITIS / BSI
- CRA (geplant ab 11/2027)

Nachweisbarkeit & Abhängigkeiten

Fehlende Transparenz

- Kritische Prozesse & Usecases
- Operative Kryptografie unbekannt
- Software-Abhängigkeiten unklar
- Zertifikate & Keys verstreut
- Algorithmen unklar

Keine belastbaren Aussagen!

Zukunft PQC

- Heute: Vorbereitung empfohlen
- Morgen: Compliance-Pflicht (2030?)
- Hohe Migrationskomplexität
- Abhängigkeiten entscheidend

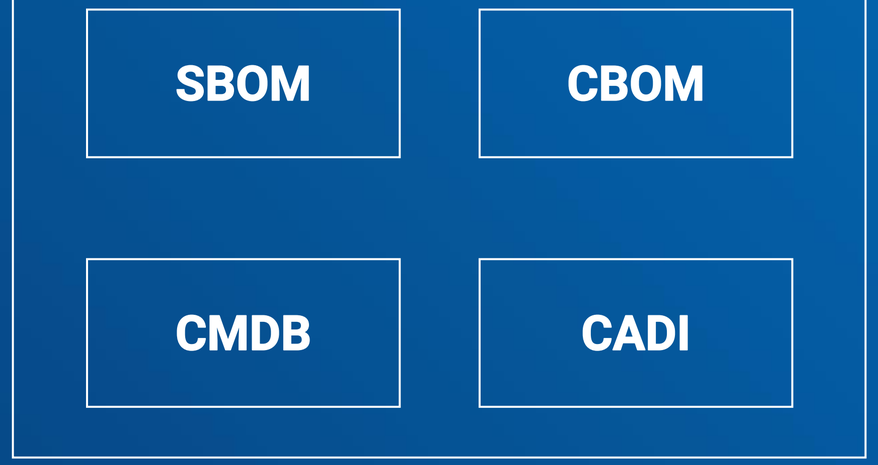
Jetzt vorbereiten!

Grundlagen der Crypto Agilität- Dynamik

Hürden heute

- Prozess & UC RM unvollständig
- Kryptografie ist dynamisch
- Keys & Certs verteilt
- CMDB statisch & manuell
- SBOM ohne Crypto-Layer

Inventar Bausteine



Erforderliche Transparenz

- Crypto-APIs & Libraries
- Operative Keys & Certs
- Algorithmen & Endpunkte
- Dynamische Abhängigkeiten

Erst die Kombination liefert ein vollständiges Bild und ermöglicht die RM basierte Umsetzung!

Automation & Algorithmen- agnostische Protokolle

Kernbestandteil für Crypto-Agilität & PQC

PQC Komplexität bedeutet:

- Größere Schlüssel & Zertifikate
- Kürzerer Lifecyle (mehr Wechsel)
- Hybrid Zertifikate (klassisch & PQC)
- Manuelle Prozesse skalieren nicht mit

Automation & Agnostik bedeutet:

- Skalierung ohne zusätzliche Manpower
- Algorithmuswechsel ohne Unterbruch möglich
- Konsistente, reproduzierbare Abläufe
- Kosten, Fehler, Störungen Reduzierung

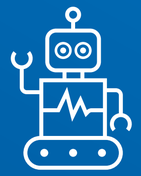
Algorithmus abhängig	Algorithmen agnostische
SCEP	EST
RPC/ DCOM (MS)	CMP / CRMF
Alle nicht PQC fähigen wie z.B.	ACME
proprietäre & legacy Protokolle	CMC
mit fester RSA / ECC Bindung	SCVP

Der Weg zur Crypto Agilität

Übersicht

- Relevante Regularien
- Kritische UC & Prozesse
- Abhängigkeiten identifizieren
- Risiken bewerten

Orientierung



Operativ

- Verantwortung & Ownership
- Crypto Assets Inventarisieren
- Einheitliche Policies umsetzen
- Lifecycle automatisieren

Umsetzung

Ziele

- Effiziente Crypto Anpassung
- Reduktion operativer Risiken
- Reduktion Business Impact
- Zukunftssichere Compliance

Ergebnis

Executive Summary –Strategische Bedeutung

- Unternehmen benötigen heute eine klare, nachweisbare Kontrolle über ihre Kryptographie. Regulatorische Anforderungen (NIS2, DORA, CRA, ISO) verschärfen diese Pflicht, während operative Transparenz über Algorithmen, Schlüssel und Abhängigkeiten in vielen Organisationen fehlt.

- Klassische Inventare reichen nicht aus. Ein vollständiges, auditfähiges Risikobild entsteht erst durch die Kombination aus CMDB, SBOM, CBOM und einem operativen CADI.

- Crypto-Agilität ist damit eine strategische Fähigkeit:
  Sie reduziert operative Risiken, stärkt die Resilienz und schafft die Grundlage für eine planbare PQC-Transformation.

Jetzt zu handeln ist entscheidend, um Compliance-Risiken und höhere Migrationsaufwände zu vermeiden!

Fragen & Antworten – Offene Diskussion

Vielen Dank !

HST GmbH
Ralph Jung

Roundtable 1: Regulatorische Einstufung & Handlungsbedarf

1. Wo fehlen uns aktuell Transparenz oder Nachweise?
2. Welche Regulatorien erzeugen für uns heute kryptografischen Handlungsbedarf?
3. Welche kryptografischen Nachweise können wir heute bereits liefern?
4. Welche Risiken entstehen daraus für Compliance, Betrieb und PQC-Readiness?
5. Welche ersten Schritte wären realistisch und kurzfristig umsetzbar?

Zusätzliche Infos & Referenzen

NIS2
Art. 21: Pflicht zu Kryptographie, Schlüsselmanagement & Asset-Inventaren
Erwägungsgründe 54/57: Kontrolle über kryptographische Verfahren & Schlüssel
Referenz: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32023L2555

DORA
EU-weit verbindliche Anforderungen an Crypto- Lifecycle & Resilienz
Gilt für Finanzsektor & kritische ICT-Dienstleister
Referenz: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32022R2554

BAIT / VAIT / KAIT
Nationale Konkretisierung der BaFin
Bleiben bestehen, werden an DORA harmonisiert
Referenz: https://www.bafin.de (→ Rundschreiben BAIT/VAIT/KAIT)

CRA (Cyber Resilience Act)
Herstellerpflichten: sichere Kryptographie, SBOM, Schwachstellenmanagement
Grundlage für CBOM-Daten & PQC-fähige Produkte
Referenz: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32024R2847

ISO 27001 / 27002
A.5.9 Asset Inventory
A.8.24 Use of Cryptography
A.8.25 Key Management
A.8.16 Monitoring Activities
Referenz: https://www.iso.org/standard/82875.html

KRITIS / KRITIS-Dachgesetz
Einsatz geeigneter Kryptographie & Resilienzpflichten
Referenz: https://www.bmi.bund.de (→ KRITIS-Dachgesetz)

DISKUSSIONSIMPULS

Was bedeutet Krypto-Agilität in der Praxis - am Beispiel Siemens

Harald Kaiblinger

CEO bei 8 Unlimited GmbH
& Consultant bei Siemens

Ralph Jung

Senior Projektmanager & Consultant
HST GmbH Technische Entwicklungen

FUTURE CONNECTIONS

CIRCLE

Powered by:

digicert

Post Quantum with Crypto Agility into the Future

UNLIMITED

IT CONSULTING & SECURITY

office@8unlimited.net

Post Quantum with Crypto Agility
into the Future

PQC - Readiness in der Praxis

Von Quantenrisiko zur Chance
Operative Umsetzung in einem weltweit agierenden Großunternehmen

UNLIMITED

Post Quantum with Crypto Agility into the Future

Post-Quantum Cryptography: the Good, the Bad, and the Powerful

The Good The Bad and The Powerful

Aktueller Stand

Quantencomputing 2026 – Relevanz steigt, aber evolutionär:

- Reale Fortschritte, aber noch kein kommerzieller Durchbruch
- Staatliche Programme treiben Entwicklung, Details bleiben unklar
- Erste kommerzielle Anwendungen existieren, aber begrenzt
- Wert & Nutzung entsteht schrittweise, nicht disruptiv

Keine Panik- aber strategisch jetzt vorbereiten!

UNLIMITED

Warum es wichtig ist

Die Bedrohung verändert und beschleunigt sich:

- Skalierbare Quantencomputer machen heutige Verschlüsselung verwundbar
- Harvest Now, Decrypt / Forge Later: „Sammel“ jetzt, entschlüssle / fälsche später
- Agentic AI: Verstärkt Angriffe und Verteidigung gleichermaßen
- Langzeitdaten besonders gefährdet IPO, Gesundheitsdaten, Verträge, Identitäten

PQC-Readiness ist eine Frage der Datenlebensdauer, nicht der Technologie!

UNLIMITED

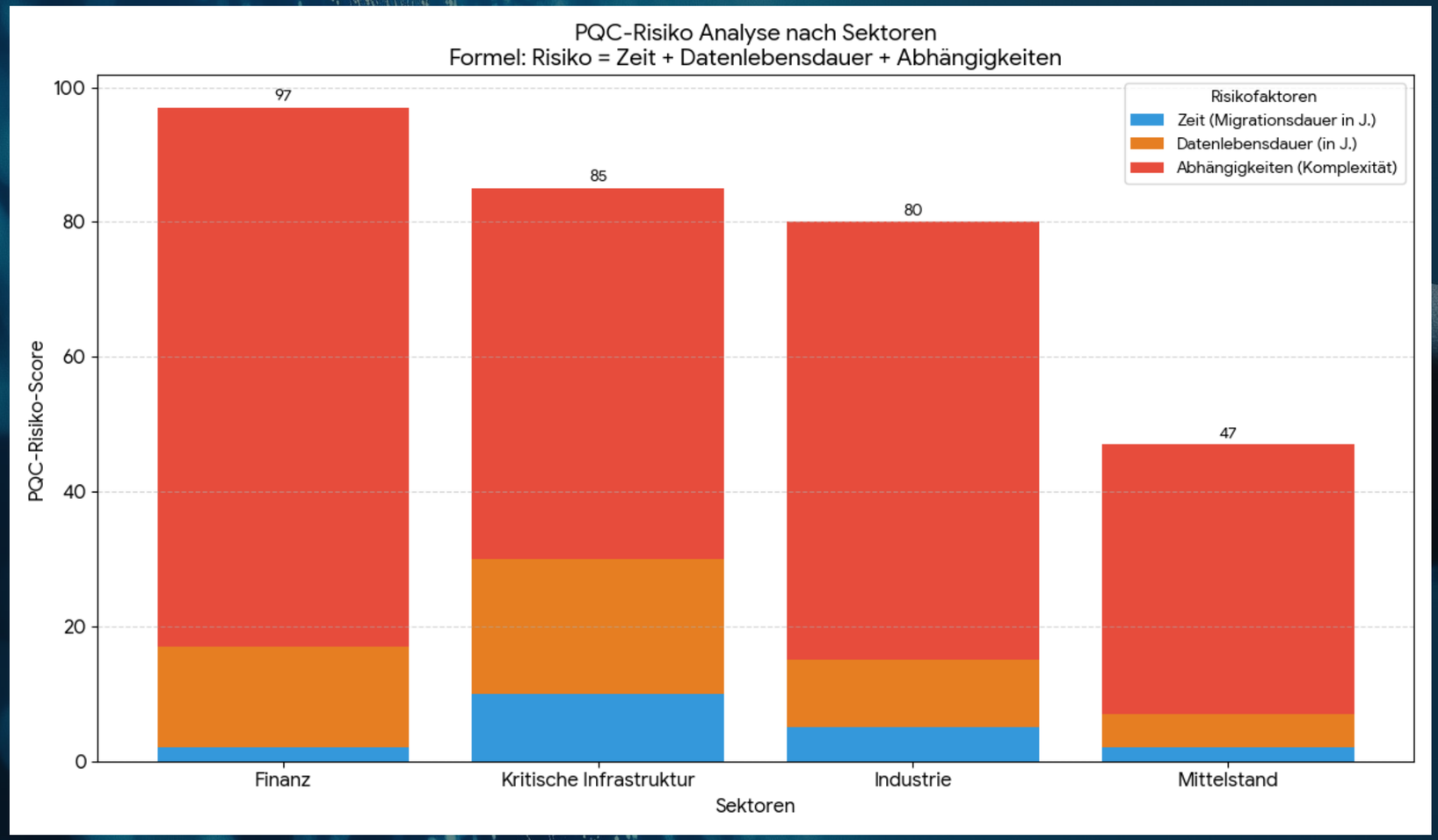
Kritische Bereiche

- Langzeitdaten & langlebige Systeme
- Lieferketten nicht quantenbereit
- Versicherungsrisiken steigen
- Regulatorischer Druck nimmt zu (NIST, NIS2, Branchenvorgaben, etc.)

PQC-Risiko = Zeit + Datenlebensdauer + Abhängigkeiten

UNLIMITED

PQC-Risiko = Zeit + Datenlebensdauer + Abhängigkeiten



Herausforderung - PQC in der Praxis

- Begrenzte Transparenz über eingesetzte Kryptographie
- Betriebsrisiken während Migrationen
- Hersteller- und Technologiefragmentierung
- Potenzielle Leistungs- und Infrastrukturauswirkungen
- Ressourcen- und Budget Beschränkungen

Nichts Neues!

UNLIMITED

PQC - Readiness in der Praxis

- Kritische Use Cases identifizieren
- Langlebige Daten & Systeme priorisieren
- Abhängigkeiten analysieren (Daten, Systeme, Lieferanten)
- PQC-Risiko pro Use Case bewerten

PQC-Readiness ist prozessgetrieben, nicht algorithmisch!

UNLIMITED

Wie Priorisierung messbar wird

Shelf-Life der Daten vs. Zeit mittels Quantum-Adjusted Risk Score
QARS & Mosca’s Theorem

- bewertet Datenlebensdauer
- bewertet Migrationsaufwand
- bewertet Bedrohungsfenster

Ergebnis: Priorisierung nach quantenrelevanter Kritikalität

PQC-Risiko wird quantifizierbar und steuerbar!

UNLIMITED

Werkzeuge & Verfahren

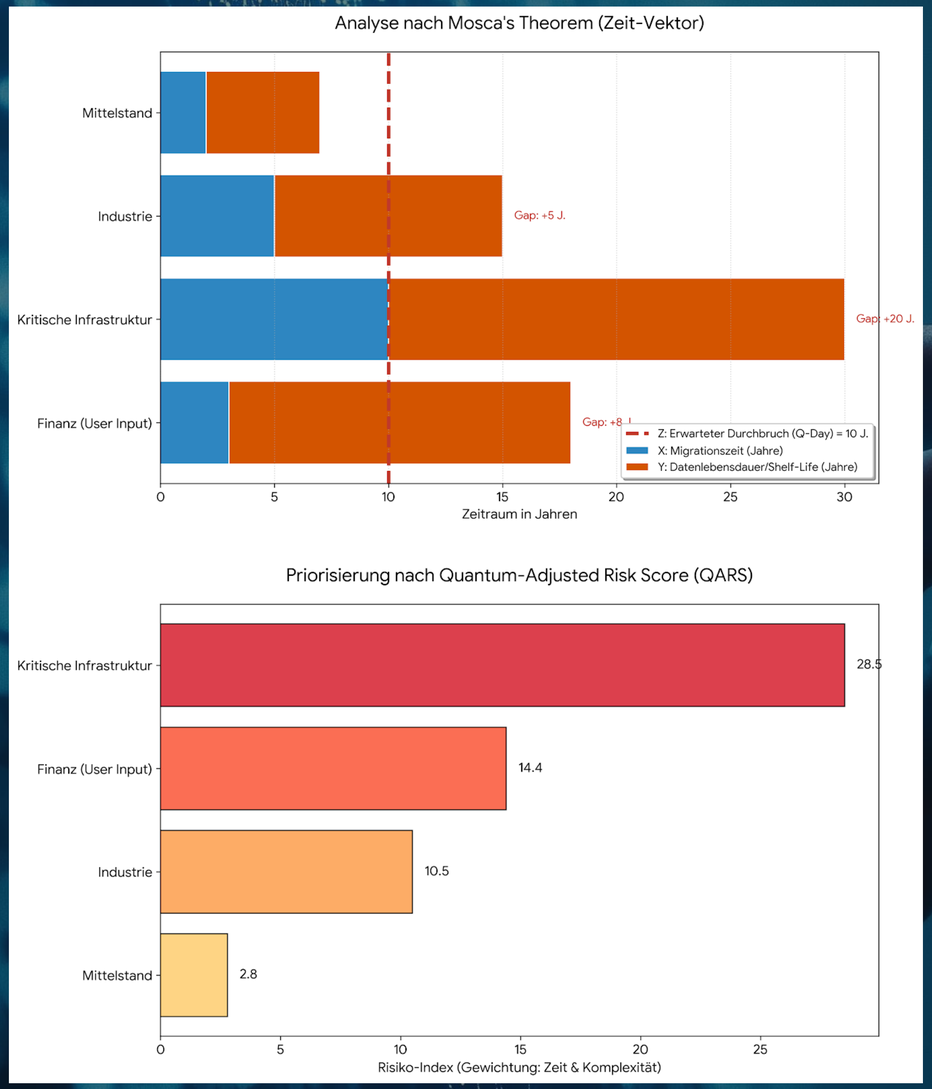
Agentenbasierte KI unterstützt die Bewertung von Mosca's Theorem, indem sie Datenlebensdauer, Migrationsaufwand und Quantenrisiko zu einem Quantum-Adjusted Risk Score (QARS) zusammenführt.

Step	Agenten basierte Aktion	Auswirkung HNDL Risiko
Inventarisierung	Kontinuierliche Erkennung von Daten „at rest" und „in transit".	Sichtbarkeit darüber, welche Daten heute abgegriffen werden könnten.
Priorisierung	Klassifizierung nach Datenlebensdauer (z. B. Finanzdaten 7 Jahre, Patente 20 Jahre).	Fokus auf Daten mit dem längsten Verwundbarkeitsfenster.
Mitigation	Automatisierte Migration langlebiger Archive in PQC-geschützte Speicher.	Reduziert den Wert bereits abgegriffener Daten für Angreifer.

QARS macht PQC-Risiken messbar und ermöglicht eine priorisierte, operative Umsetzung.

UNLIMITED

Agentenbasierte KI unterstützt die Bewertung von Mosca’s Theorem, indem sie Datenlebensdauer, Migrationsaufwand und Quantenrisiko zu einem Quantum-Adjusted Risk Score (QARS) zusammenführt.



Kernbotschaften

- PQC ist eine strategische Transformation
- Crypto-Agilität ist Voraussetzung, keine Option
- Proaktive Umsetzung reduziert Kosten, Risiken und Betriebsstörungen
- Unternehmen, die heute handeln, sichern ihre digitale Souveränität

Prokrastination ist keine Lösung!

Fragen und Antworten- offene Diskussion

Vielen Dank !

UNLIMITED

Roundtable 2: PQC-Readiness operativ umsetzen

Von der Theorie zur operativen Priorisierung.

30-40 Minuten

1. Welche unserer Use Cases haben die längste Datenlebensdauer?
2. Welche Systeme sind schwer migrierbar?
3. Welche Daten wären bei einem HNDL/HNFL-Szenario am geschäftskritischsten?
4. Welche Abhängigkeiten bestimmen die Prioritäten unserer Use Cases?
5. Was wären die nächsten Schritte?
6. Welche Voraussetzungen sind nötig um PQC als Prozess zu etablieren?

UNLIMITED

PKI Consortium

Wir sind eine vielfältige Gruppe von 300+ Organisationen wie Regierungen, Wirtschaftsprüfern, Beratern, Vertrauensdienstleistern sowie Software- und Hardwareanbietern

Wir sind eine gemeinnützige Organisation, ohne Mitgliedsbeiträge

Unsere Vision ist "Vertrauenswürdige digitale Vermögenswerte und Kommunikation für alle und alles".

pkic.org

UNLIMITED

IT CONSULTING & SECURITY

Post Quantum into the Future

https://www.linkedin.com/in/kaiblinger/

office@8unlimited.net

UNLIMITED

IT CONSULTING & SECURITY

CLOSING

Lessons learned und
Zusammenfassung der Erkenntnisse
des Nachmittags

Leonhard Roschlau

Business Unit
Manager
LSZ Future
Connections

Christian Müller

Regional Vice
President
DigiCert

FUTURE CONNECTIONS
CIRCLE

Powered by:
digicert


FUTURE CONNECTIONS
CIRCLE
Powered by:
digicert