QUANT-X SECURITY & CODING

Quantentechnologien - Neue Aspekte für IT Sicherheit

https://quant-x-sec.com/ | consulting@quant-x-sec.com

Unser Service: Beratung und Auftragsentwicklungen in

https://quant-x-sec.com/ | consulting@quant-x-sec.com

Referenzen

IT Sicherheitsprojekte

- Integration eines Fintechs in eine internationale Bank (ISMS)
- Kryptografisches Zertifikatsmanagement
- IAM Platform Analyse
- SIEM

Quanten-Aktivitäten

- Quantensicherheitsanalysen
- Anträge für Quantensicherheitsprojekte in Konsortien auf Bundes- und EU Ebene
- Assoziiertes Mitglied des QUIC
- Mitglied des QBN

https://quant-x-sec.com/ | consulting@quant-x-sec.com

Quantentechnologien - Ein Traum?

QRNG
Quantum Random Number Generator. Erzeugt idealerweise echte Zufallswerte.

Quanten Kommunikation
Aka Quantum Key Distribution. Schlüsselaustausch auf quantenmechanischen Prinzipien.

Quantum Sensing und Metrologie
Hochpräzise Messungen mit Hilfe von quantenmechanischen Effekten.

Quantum Imaging
Erweiterung von Quantum Sensing. Hochauflösende Abbildung eines Objekts mit quantenmechanischen Effekten.

Quanten Simulation
Simulation zur Lösung eines spezifischen Problems

Quantum Computing

- Quantum Annealing (für wenige Klassen von Problemen)

Quantentechnologien - Ein Traum?

QRNG
Quantum Random Number Generator. Erzeugt idealerweise echte Zufallswerte.

Quanten Kommunikation
Aka Quantum Key Distribution. Schlüsselaustausch auf quantenmechanischen Prinzipien.

Quantum Sensing und Metrologie
Hochpräzise Messungen mit Hilfe von quantenmechanischen Effekten.

Quantum Imaging
Erweiterung von Quantum Sensing. Hochauflösende Abbildung eines Objekts mit quantenmechanischen Effekten.

Quanten Simulation
Simulation zur Lösung eines spezifischen Problems

Quantum Computing

- Quantum Annealing (für eine Klasse von Problemen)

Kommerzieller QKD Transfer in Wien seit 2004

Kommerzielle Anwendung in QKD Geräten

Tests für Militär und Medizinische Anwendungen

Protein Folding / Materialwissenschaften

D-Wave's Advantage > 5000 qubits

Google, IBM, Terraquantum, Quantinuum, …

Informationssicherheit - Bereiche

Configuration Management:

What do we need to protect?

Information Risk Management:

How do we to protect our assets?

Platform/Infrastructure Security

System and network security by design.

Identity Access Management

Access control by design.

Change Management

Stay safe when changing code, systems and infrastructure.

Operational Resilience

Fallback solutions and quick recovery.

Security Monitoring

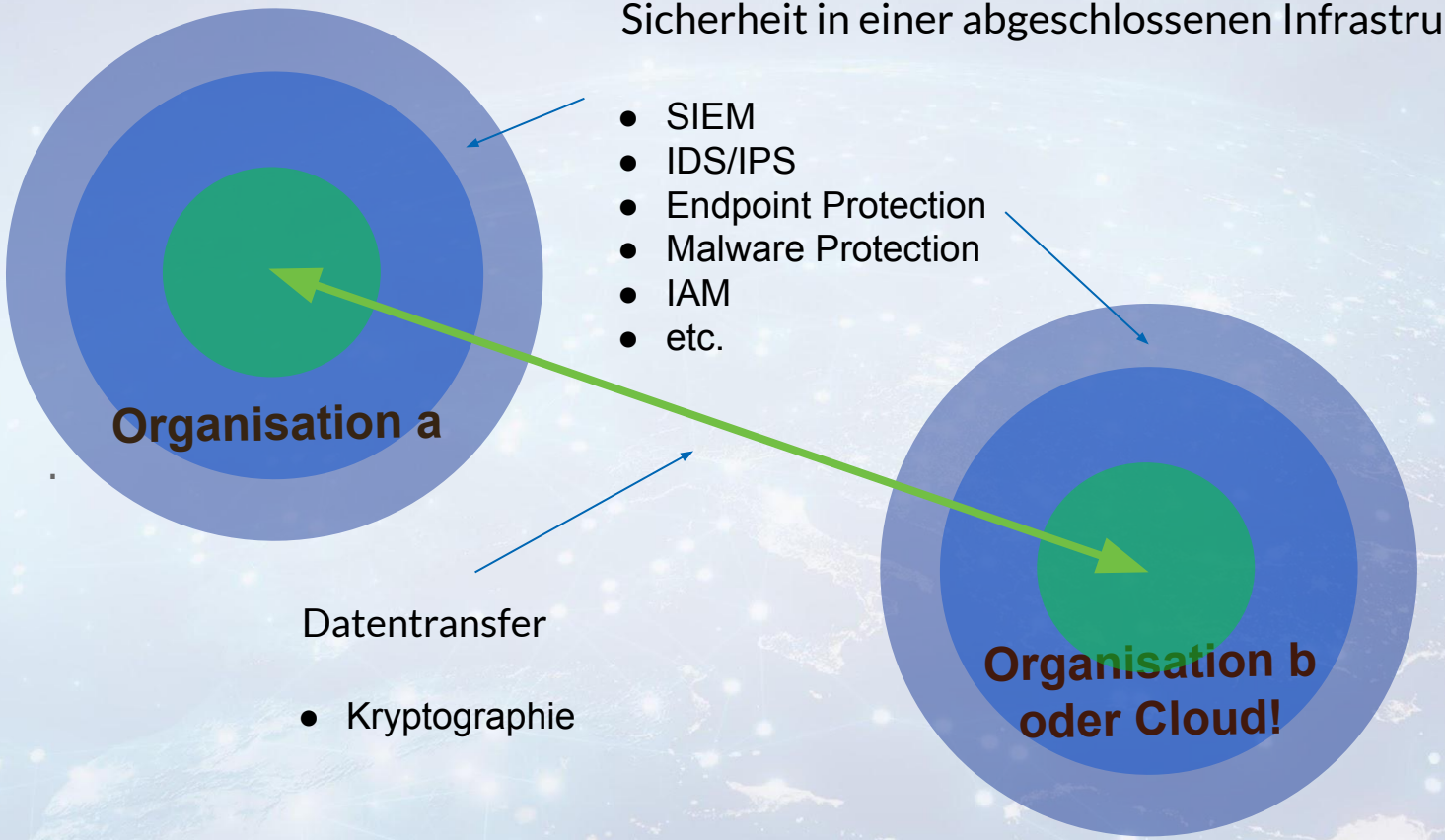
Monitor and react in time.

Cybercrime Resilience

React swiftly and adjust your security.

https://quant-x-sec.com/ | consulting@quant-x-sec.com

Sonderstellung Kryptografie



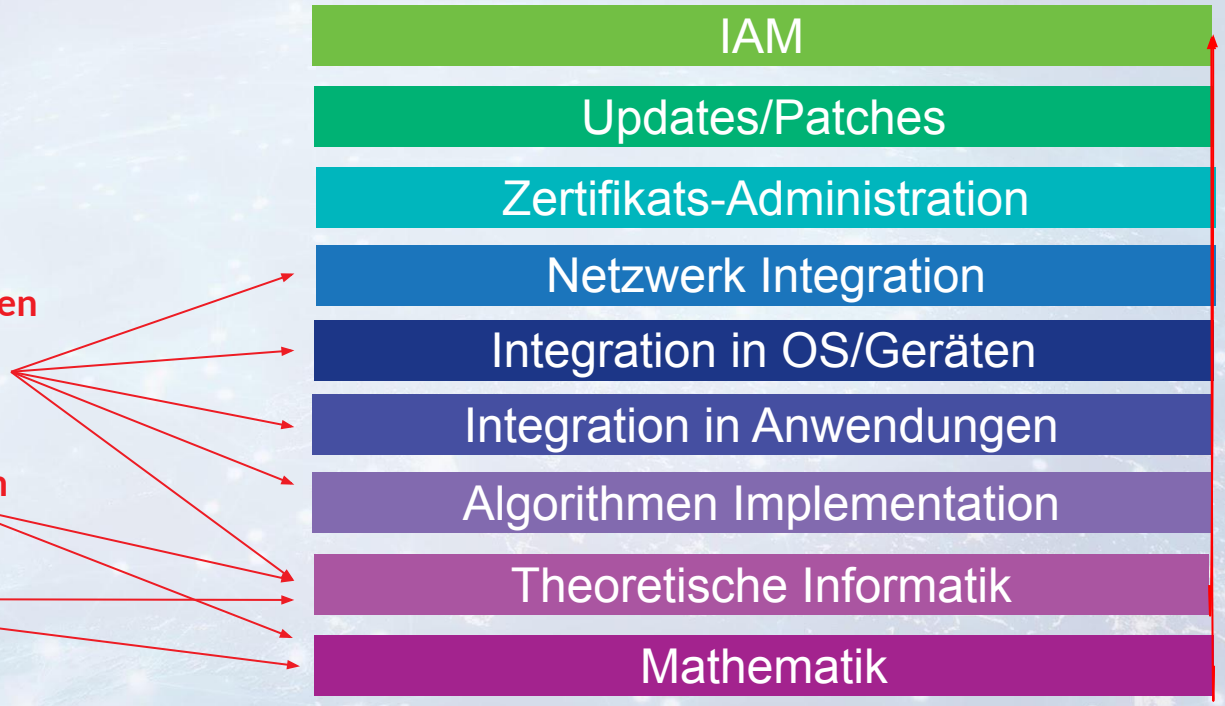
Bedrohungen durch Quantentechnologien

BEDROHUNGEN

High Performance Anwendungen (Binäre Technologien)

Neue Mathematische Lösungen

Quantum Computing



https://quant-x-sec.com/ | consulting@quant-x-sec.com

Bedrohungen durch Quantentechnologien

Quantenprozessoren werden Entschlüsselung (full cryptanalysis) von verschlüsselten Daten ermöglichen. *Betroffen sind u. a.*:

Verschlüsselung	**Quantenangriff**	**Maßnahmen**
Diffie-Hellmann	Shor	PQCrypto, QKD
RSA	Shor	PQCrypto, QKD
Elliptische Kurven	Shor	PQCrypto, QKD
AES-128	Grover's Search	AES-256

Wann ist es soweit?

- Unterschiedliche Einschätzungen von Experten
- NIST, BSI und andere Behörden empfehlen, unabhängig von dieser Frage mit Migration zu Post-Quanten Sicherheit zu beginnen

https://quant-x-sec.com/ | consulting@quant-x-sec.com

Handlungsempfehlungen / Roadmaps

Handlungsempfehlungen / Roadmaps

1. BSI: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Post-Quanten-Kryptografie.pdf
2. NIST: https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3-submissions)
3. ANSSI: https://www.ssi.gouv.fr/publication/anssi-views-on-the-post-quantum-cryptography-transition/

Information zu Quanten Kommunikation/QKD

Es gibt weltweit seit vielen Jahren etablierte QKD Netzwerke, z. B. QUESS: 2000km quantum communication channel between Shanghai and Bejing, SwissQuantum, SECQC Austria, Tokyo QDK Network, DARPA USA. Es gibt jedoch noch keine vom BSI zertifizierte oder zugelassene QRNG und QKD Geräte- Mehr Information zu Empfehlungen des BSI und der NIST:

- BSI | Quantenkryptografie
- NIST | Quantum Networks

Warum unabhängig vom Tempo der Quanten-Entwicklungen handeln?

Weiteren Bedrohungen vorbeugen

- Passwort und Krypto Cracking Tools (Hashcat und ähnliche Tools)
- Aggregierte Computing Ressourcen und Parallelisierung von Angriffs-Prozessen
- Neue mathematische Lösungen betreffen Parameter und Konfiguration von klassischer Kryptografie

Auswirkungen

Die Folgen des Eintritts von Quantenbedrohungen sind katastrophal! Die Entwicklung von Quantenprozessoren wird von Experten als “internationales Kriegsrennen” bezeichnet.

Außerdem:

- Datensammler können in der Vergangenheit gesammelte Daten entschlüsseln, wenn entsprechende Quantenprozessoren verfügbar sind.
- Migrationen können Jahre dauern.

Quant-X Service für Quanten-Sicherheit

“Bewahrung der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit aktuell transportierter Daten – auch in ferner Zukunft!”

Unsere Expertise

- Risikoassessments mit Quanten-Bedrohungsszenarien
- Integration von Quantensicherheit in bestehende Infrastrukturen und Systeme
- Quanten Sicherheits-Analysen von Systemen und Algorithmen
- Sicherheitsbeweise und Nachweise von Geräten

Wir unterstützen auch gerne andere Consulting Firmen mit spezifischem Knowledge Transfer.

https://quant-x-sec.com/ | consulting@quant-x-sec.com

Open Source Projekt

Untersuchung offener Fragen in Post-Quanten Sicherheit:

https://github.com/Quant-X-Security-Coding-GmbH/QAA_Condition_Number

Industrial Speaker for

Fachgruppe Computeralgebra

Co-Organisation of *Industrial Computeralgebra Conference with Focus Cryptography*

Memberships and Associations

Gesellschaft für Informatik

Deutsche Mathematiker-Vereinigung

European Mathematical Society

Quantum Business Network

Member of QBN

European Quantum Flagship

https://quant-x-sec.com/ | consulting@quant-x-sec.com

Fazit

Legen Sie los mit Integration von Post-Quanten und Quanten Sicherheit!

Vielen Dank fürs Zuhören!!!

Unsere Webseite: https://quant-x-sec.com/
Slides: https://quant-x-sec.com/published.htm