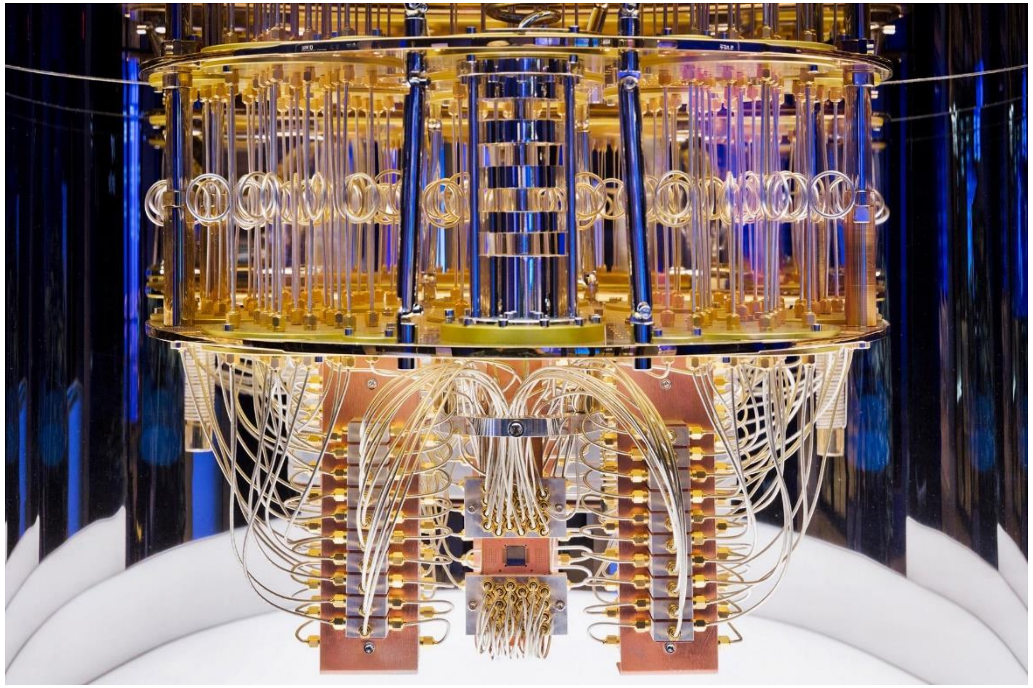
TeleTrusT-EBCA "PKI-Workshop" 2022

Berlin, 29.09.2022

Cybersecurity Approach to protect Products and Services in a PQ World

Anna Katharina Lindner, Siemens

Quantum Computers will break current Cryptography



IBM’s 27 Qubit System in Ehningen

- Rapid developments in the last 30 years
- Prominent quantum algorithms:
  - □ Shor‘s allows facorization of big numbers into prime factors
  - □ Grover‘s allows efficient searches in unsorted lists
- Millions of qubits needed to break asymmetric algorithms

Post Quantum Cryptography

- Quantum resistant cryptographic algorithms are the future
- NIST is working on new standards since 2016:
  - CRYSTALS-KYBER (PK)
  - CRYSTALS-Dilithium
  - FALCON
  - SPHINCS+

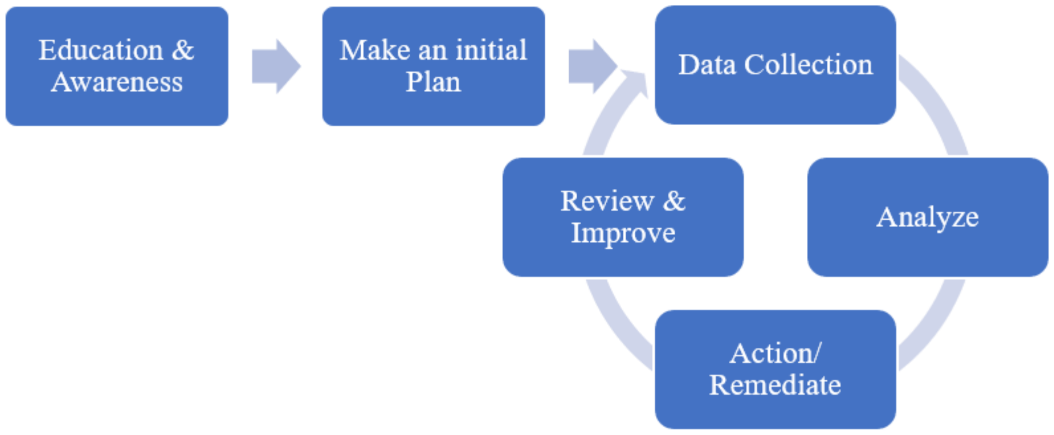
- All new algorithms have significant drawbacks

Cryptography in a PQ Era

- Resulting question:
  - How does an organization get PQ ready?

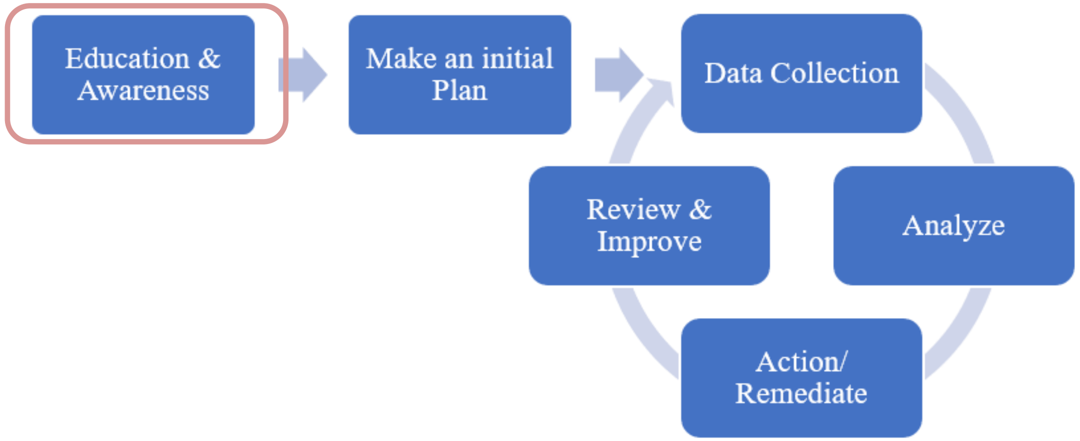
- The answer:
  - Through a cryptographic migration

A Crypto Migration Framework in 6 Phases



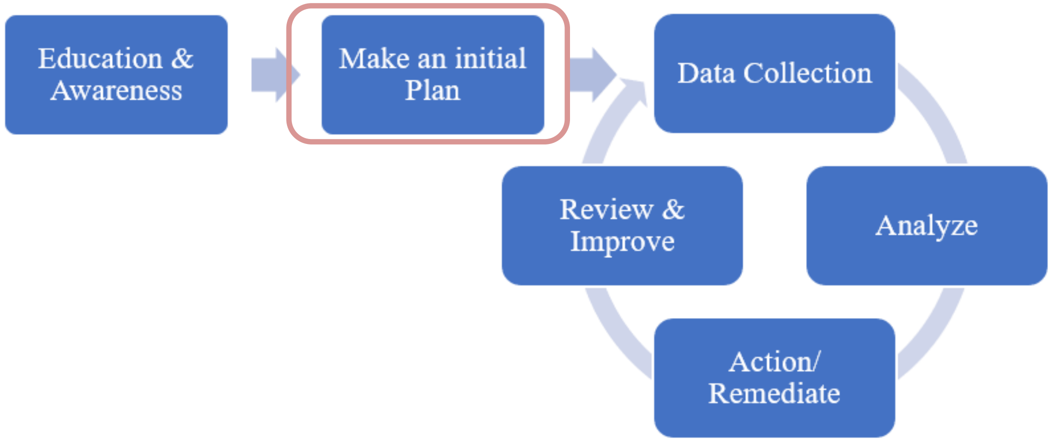
- A practical migration plan
- Most common approaches and strategies combined

A Crypto Migration Framework in 6 Phases – Phase 1



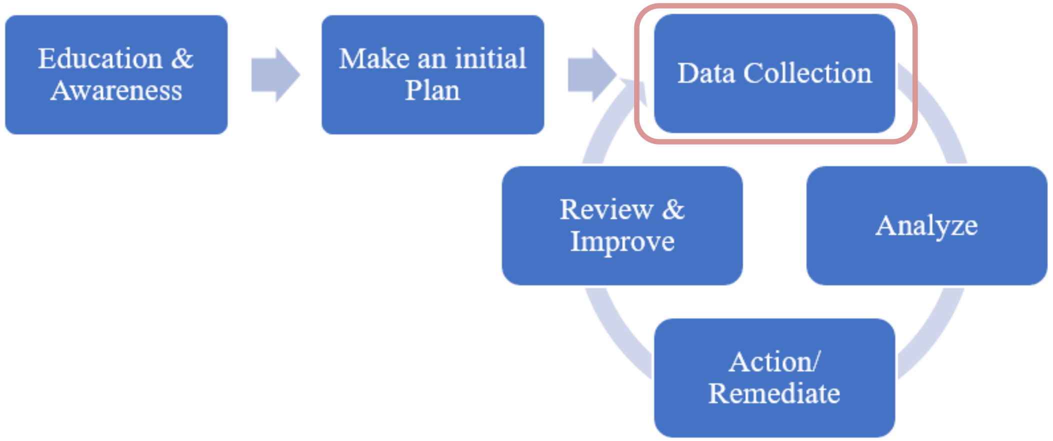
- Phase 1: Awareness
  - □ Educate yourself
  - □ Raise awareness within management
  - □ Publish ressources for colleagues

A Crypto Migration Framework in 6 Phases – Phase 2



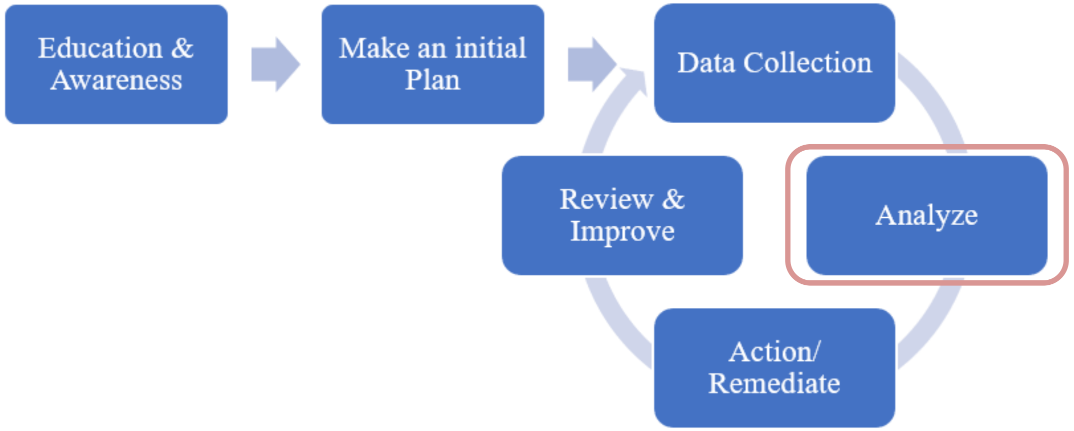
- Phase 2: Make an initial Plan
  - □ Form a project team
  - □ Perform a risk analysis
  - □ Determine the migration goal
  - □ Determine a timeline & emergency timeline

A Crypto Migration Framework in 6 Phases – Phase 3



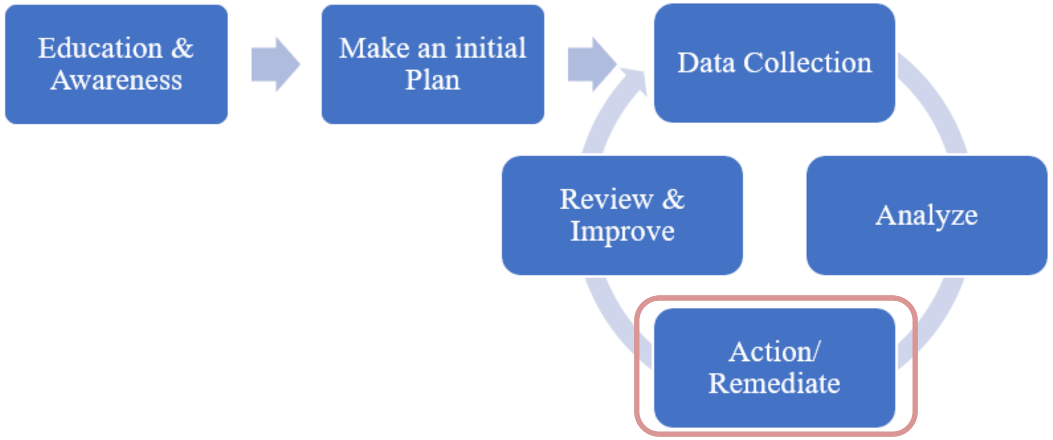
- Phase 3: Data Collection
  - □ Check for useful starting databases
  - □ Plan the structure for a cryptographic inventory
  - □ Locate assets
  - □ Add assets to inventory
  - □ Identifiy policies and standards that need to be updated

A Crypto Migration Framework in 6 Phases – Phase 4



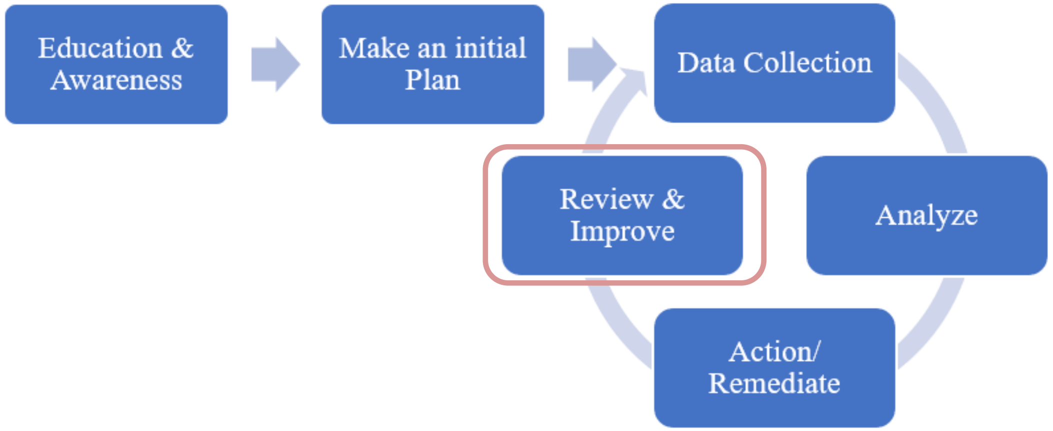
- Phase 4: Analyze
  - □ Identify levels of crypto agility and PQ readiness
  - □ Determine remediations
  - □ Prioritize assets
  - □ For third-party assets:
    - Determine a vendors PQ-strategy
    - Find replacements
  - □ Document the state of the asset

A Crypto Migration Framework in 6 Phases – Phase 5



- Phase 5: Action
  - □ Apply mitigations
  - □ Update documentation
  - □ Update Policies
  - □ Test solutions

A Crypto Migration Framework in 6 Phases – Phase 6



- Phase 6: Review
  - □ Quantify improvements in PQ readiness and crypto agility of assets
  - □ Review migration process
  - □ Adjust the initial plan accordingly
  - □ Add new assets to the inventory

Sources

- Literature:
  - □ “Cryptography Apocalypse“ by Roger A. Grimes
  - □ “Practical Preparations for the Post-Quantum World” by CSA
  - □ “Migration strategies and recommendations to Quantum Safe schemes” by ETSI

Questions?

Thank you for your attention.