TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

TeleTrusT-interner Workshop

Berlin, 26. - 27.06.2024

"Kryptoagilität"

Dr. Tobias Fehenberger, Adva Network Security, Leiter der TeleTrusT-AG "Kryptoagilität"

Adva
NETWORK SECURITY

Kryptoagilität

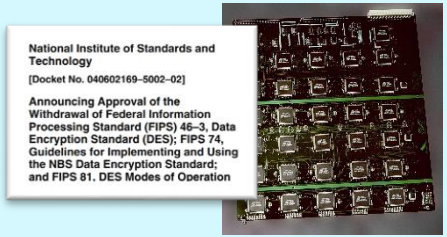
Langfristige Sicherheit von IT-Systemen

TeleTrusT Interner Workshop | Berlin | 27. Juni 2024 | Tobias Fehenberger

Angriffe auf Kryptografie

Brute-force

1998: Deep Crack breaks DES

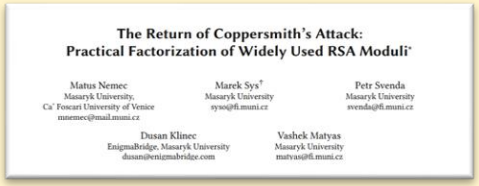


Mathematische Angriffe

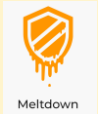
Source: arstechnica.com/information-technology/2022/08/sike-once-a-post-quantum-encryption-contender-is-koed-in-nist-smackdown/

Implementierung

2017



2017



2016

Konfiguration / Patching

2024

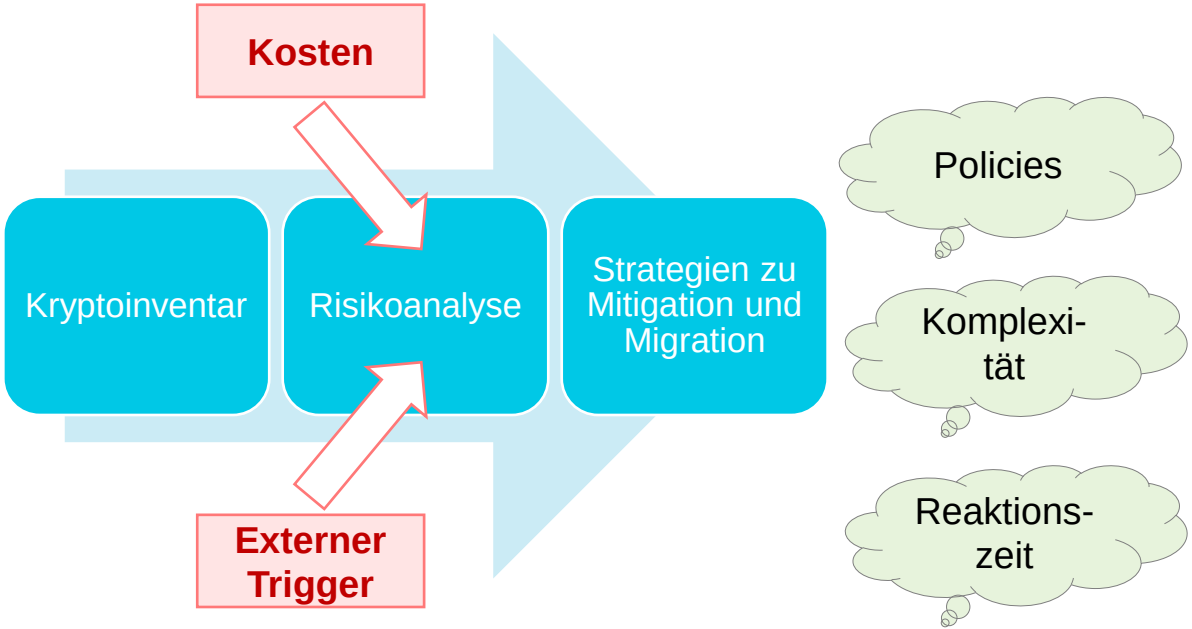
Kryptografie ist allgegenwärtig – und wird ständig gebrochen

Definition Kryptoagilität

Kryptoagilität beschreibt einen unternehmensweiten Prozess bei Herstellern und Anwendern von IT-Systemen, bei dem als Reaktion auf externe Einflüsse sicherheitsrelevante Bestandteile eines IT-Systems ausgetauscht werden, ohne dass Kernfunktionalitäten beeinträchtigt werden.

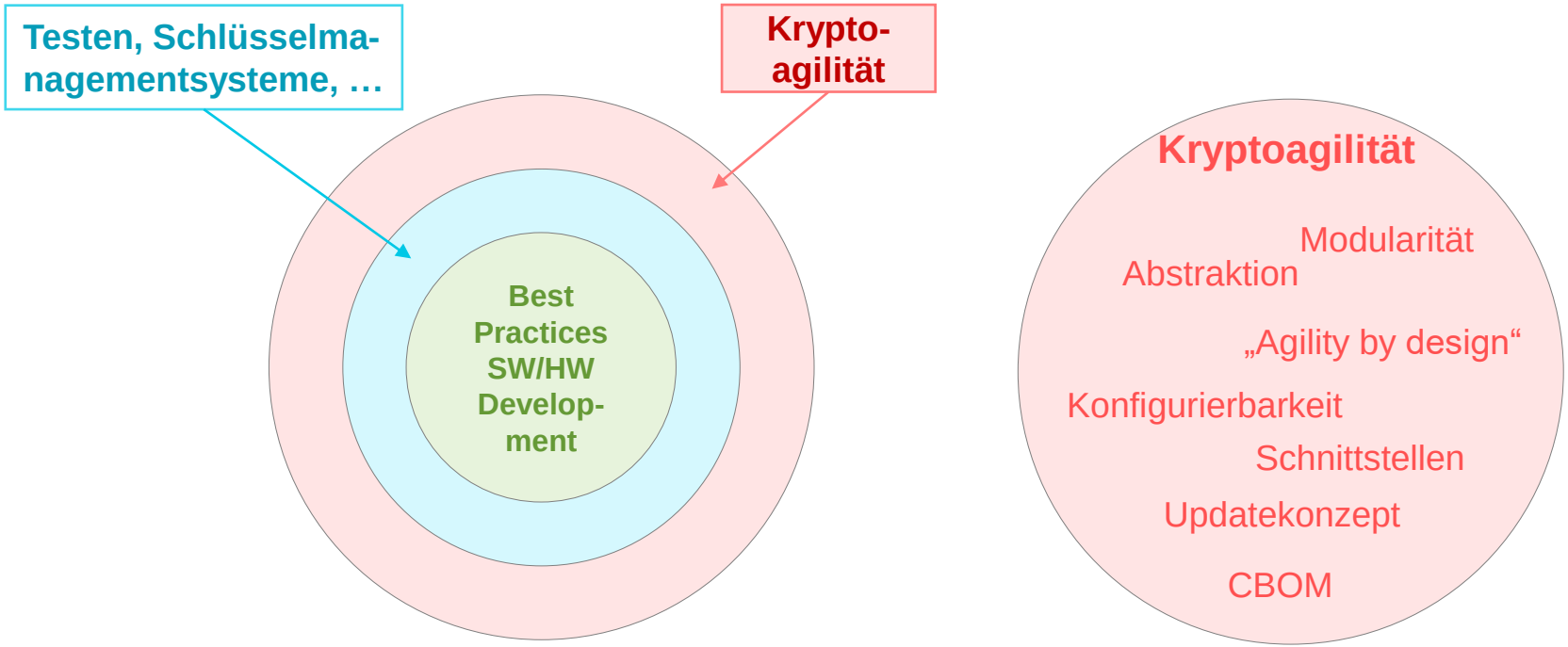
Viel mehr als ein Software-Update!

Vorbereitende Maßnahmen



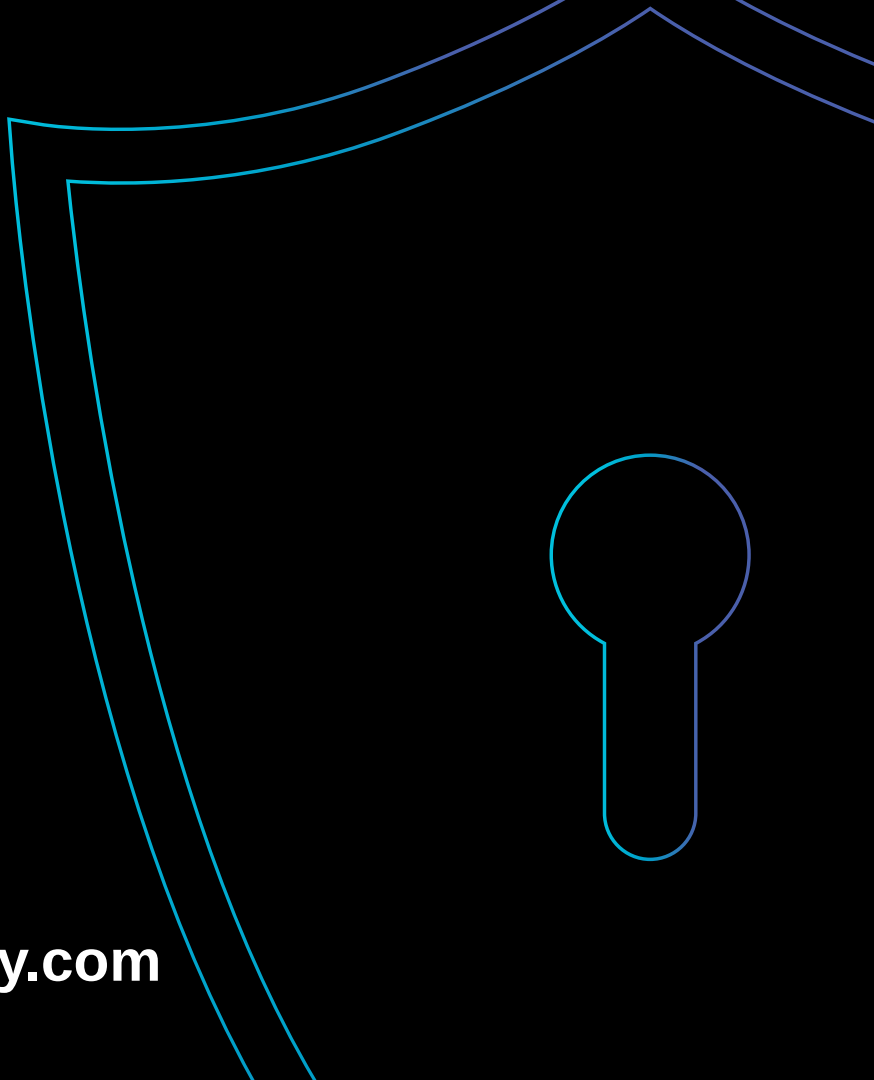
Prozessdenken ist entscheidend für Kryptoagilität

Technische Umsetzung [Hersteller]



Komplexe Design- und Entwicklungsvorgaben für Hersteller

Danke an die AG Kryptoagilität



tobias.fehenberger@advasecurity.com