Kvantová odolnost a bezpečnost

Alanata TALKS

sympulse

AGENDA

Úvod

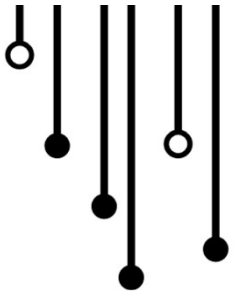
- Kvantová bezpečnost je zásadní v éře kvantových počítačů, které mohou prolomit současné šifrovací standardy.
- Tato prezentace popisuje přístup k post-kvantovému šifrování (PQC) a kvantové odolnosti.
- Zahrnuje postupy, **jak se na příchod kvantových počítačů připravit**, včetně časových odhadů.
- Firma **Sympulse** využívá doporučení a své zkušenosti pro specifická prostředí zákazníků.

01

Kvantový svět

sympulse

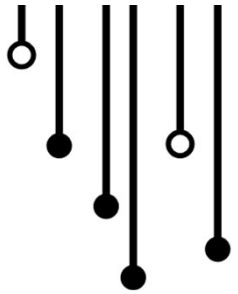
Kvantová hrozba



- Kvantové počítače nenahradí klasické počítače, ale nabídnou **zásadní výhody v kryptoanalýze**.
- Většina asymetrických šifer bude prolomena kvantovými algoritmy jako **Shorův algoritmus**.
  - Asymetrické šifrování se velké míře používá pro komunikace přes internet (data on move), jedná se o pojmy na veřejný klíč, digitální podpisy, PKI
- Symetrické šifrování **bude oslabeno např. Groverovým algoritmem**, pokud nebudou klíče dostatečně dlouhé.
  - Symetrické se používá například pro šifrování disků, dokumentů, apod. (data in rest)
- Hrozba: „**posbírej nyní, rozšifruj později**“ (z anglického harvest now, decrypt later, HNDL)
  - kde útočníci již dnes získávají šifrovaná data a rozšifrují je později s kvantovými počítači.

sympulse

Ohrožené šifrovací algoritmy

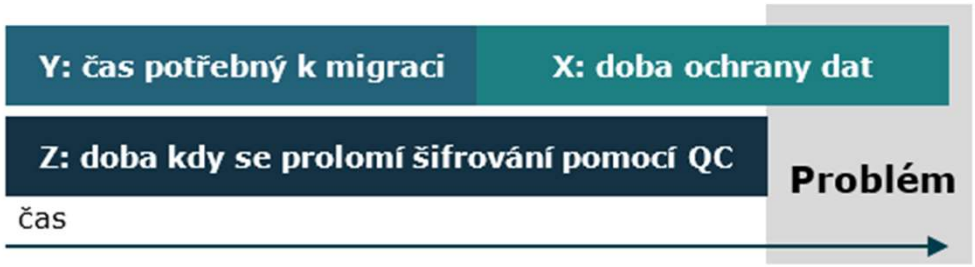


- **Asymetrické šifrování** pod hrozbou **Shorova algoritmu**
  - **Digitální podpisy** (např. DSA, EC-DSA, RSA-PSS) **i distribuce šifrovacích klíčů (KEM)** (např. DH, SCDH, ECIES-KEM, PSEC-KEM, RSA-KEM)
- **Symetrické šifrování** pod hrozbou **Groverova algoritmu**
  - **Blokové symetrické šifrování** (např. AES, Camellia, Serpent)
  - Nejde o prolomení, ale algoritmus zrychluje brute-force útoky
- **Hashe** pod hrozbou **BHT algoritmu**
  - Např. SHA, SHA3, SHAKE, Whirlpool, BLAKE2
  - Zrychluje hledání kolizí v hashovacích funkcích, což může ohrozit integritu dat.
- I když jsou tyto algoritmy zatím náročné na výkon, probíhá jejich optimalizace a zvyšování škálovatelnosti. Podobně se z druhé strany vyvíjejí a škálují i kvantové počítače.

sympulse

Kdy se obávat kvantové hrozby

- **Pokud máte citlivá data**, která potřebují být utajena více než 10 let, **je nutné se začít obávat již nyní**.
  - Kvůli HNDL (retrospektivním) útokům.
- Pro ostatní se riziko stanovuje pomocí **Moscova teorému**, který poměřuje riziko prolomení s vývojem kvantových technologií

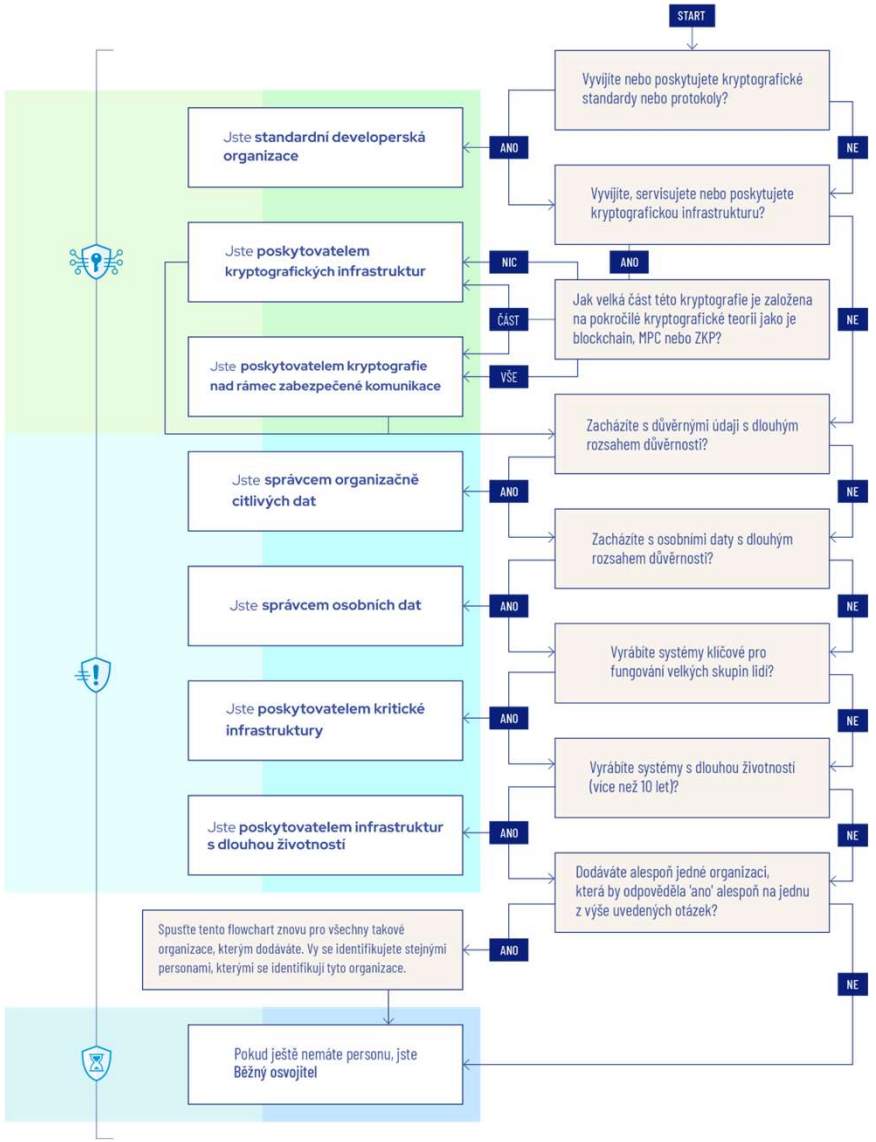


- Pokud $X+Y>Z$, kde Z je v rozsahu 8-15 let, pak je potřeba začít s protiopatřeními co nejdříve.

Jak zjistit svůj stav

Naléhavost osvojení rozdělujeme do 3 kategorií:

- Poskytovatel Kryptografické Infrastruktury
- Naléhavý Osvojitel
- Běžný Osvojitel



Zdroj: The PQC Migration Handbook, https://publications.tno.nl/publication/34641918/oicFLj/attema-2023-pqc.pdf

Musím jednat hned?

- **Pro některé je to již nyní povinné**
- Pokud mám vysoce citlivá data a „sesbírej nyní, rozšifruj později“ je pro mě velmi relevantní (identifikace relevantních dat a detekce míst možného útoku na tyto data)
- Potřebuji identifikovat skupiny a bezpečnostní zóny, které budou řešeny první (stanovení priorit)
- Monitorování/vyžádání roadmapy připravenosti klíčových vendorů v mém prostředí
- Jen příprava zabere vyšší počty měsíců
- Pokud kupuji nyní něco, co u mě bude běžet velmi dlouho ověřím, zda lze zohlednit připravenost ke kvantové odolnosti v technickém řešení nových projektů
- Začlenění do strategických záměrů, rozpočtu a kapacitního plánu zdrojů na následující roky
- Sestavení Master Plánu pro cestu ke kvantové odolnosti (jednat s rozmyslem, mít všechny potřebná data k rozhodování)
- **Připravit se, abych byl připraven**

sympulse

02

Opatření proti kvantové hrozbě

sympulse

Opatření proti kvantovým útokům

- 3 základní strategie obrany:
  - **Zdvojnásobení délky** klíčů u symetrických šifer a hashovacích funkcí.
  - Nové **Post-kvantové šifrování (PQC)**, které využívá algoritmy odolné vůči kvantovým útokům.
  - Kvantové šifrování s **kvantovou distribucí klíčů (QKD)**, což je zatím považováno za neprolomitelné, ale je drahé a omezené v použití.
- Do budoucna se očekává rozvoj kvantového internetu, který přinese další bezpečnostní služby.
- Základní otázkou ale je: kde všude šifrování moje společnost využívá a kde pro mě slabé šifrování představuje hrozbu

Post-kvantové šifrování (PQC)

- Post-kvantové šifrování (PQC) jsou kryptografické algoritmy navržené tak, aby byly odolné vůči kvantovým útokům.
- Využívají matematické problémy, které i kvantové počítače nedokážou efektivně řešit.
- Hybridní algoritmy kombinují současné asymetrické šifry s PQC pro vyšší bezpečnost do doby, než se zcela přejde na PQC.
- Symetrické šifry a hashovací funkce jsou s delšími klíči stále odolné vůči kvantovým útokům.

Situace ve světě s PQC

- **USA**
  - NIST již standardizoval první tři PQC algoritmy (ML-KEM, ML-DSA a SLH-DSA) a další jsou na cestě (Falcon, HQC).
  - NIST již má draft standardu pro přechod na PQC. Staré algoritmy budou nepodporované od 2030 a zakázané od 2035. Některé systémy už musí být post-kvantové od 2025.
  - Spojené státy kladou důraz na přechod k novým algoritmům a hybridním přístupům.
- **Evropa**
  - Státy jako UK, Francie a Německo podporují různé hybridní šifry a PQC algoritmy
  - UK již stanovilo termín a úplný přechod na post-kvantové řešení na 2035
  - Snaha koordinovat doporučení ze strany Evropské komise
  - Oficiálně žádná evropská země zatím nepodporuje kvantovou distribuci klíčů (QKD).

sympulse

Situace v ČR – NÚKIB - doporučení

- NÚKIB si hrozbu uvědomuje a již vydal obecné doporučení.
- Povinné subjekty dle zákona o kybernetické bezpečnosti **musí** dle § 26 písm. d) vyhlášky č. 82/2018 Sb. o kybernetické bezpečnosti **tato doporučení zohlednit**. Taktéž je tento dokument **závazný** pro poskytovatele eGovernment cloudu (pravidlo 7.3).
- NÚKIB odhaduje nutnost přechodu na PQC do 2027 pro citlivé informace kritické úrovně

Navrhované změny:

- Symetrické algoritmy - blokové a proudové šifry
  - AES, Camellia, Serpent
  - **Délka klíče minimálně 256 bitů**
- Klasické asymetrické algoritmy – **všechny budou odstaveny**
  - Podpisy: ~~DSA, EC-DSA, RSA-PSS, EC-Schnorr~~
  - KEM: ~~DH, SCDH, ECIES-KEM, PSEC-KEM, ACE-KEM, RSA-OAEP, RSA-KEM~~
- Post-kvantové algoritmy
  - Hybridní: ML-KEM-1024/768, FrodoKEM-1344/976, FrodoKEM-976, mcelieceXXX + klasický
  - Čistý PQC KEM: ML-KEM-1025 (CRYSTALS-Kyber) úrovně 5
  - Podpisy: LMS, XMSS, ML-DSA-87, SLH-DSA
  - Hybridní podpisy: ML-DSA, SLH-DSA, Falcon + klasický
- Hashe
  - SHA, SHA3, SHAKE, Whirlpool, BLAKE2
  - **Délka hashe minimálně 384 bitů**

sympulse

Situace v SK - NBÚ

- Úzká spolupráce s NÚKIB
- Přijetí směrnice NIS2
- Indikace, že doporučení na kvantovou bezpečnost budou obdobná jako v ČR

sympulse

Certifikát: se zaměřením na zajištění opatření ke kvantové hrozbě

- **ISO 27001:2022**
  - Širší rámec zaměřený na řízení systému informační bezpečnosti (ISMS).
  - Důraz na řízení rizik a splnění mezinárodně uznávaných bezpečnostních standardů.
- **CIS Controls v8.1 (2024)**
  - Nejlepší vžitá praxe, praktické pokyny, jak zabezpečit IT systémy a data proti kyberhrozbám.
  - Důraz na rychlá vítězství („quick wins“) a prioritizované akce.
- **Kryptografická agilita**
  - Politiky informační bezpečnosti
  - Procesy správy aktiv, konfigurací, záplat, změn
  - Technologie správy kryptografických aktiv
  - Abstrakce kryptografických funkcí při vývoji aplikací
  - Podpora použití více algoritmů nebo skupin jejich parametrů současně
  - Hardwarová kompatibilita
  - Sledování vývoje standardů, požadavků, doporučení


Certifikát č.: 2501151468

tayllorcox.com
ensure your certification

Certifikát

Systém managementu bezpečnosti informací
se zaměřením na zajištění opatření ke kvantové hrozbě

[redacted]

byl prověřen a shledán shodným s požadavky normy

ISO/IEC 27001:2022 ve spojení
s CIS CONTROLS 8.1

pro následující rozsah služeb a činností:

Vývoj a prodej software včetně zajištění veškerých souvisejících služeb a dodávek produktů třetích stran. Zajištění IT profesionálů podle požadavků zákazníků potřebných pro vývoj, implementaci a řízení projektů v oblasti informačních systémů.

Datum prvotní certifikace:	15. 01. 2025
Datum současného certifikačního cyklu:	15. 01. 2025
Platnost certifikátu do:	14. 01. 2028

Ing. Radek Nedvěd
Vedoucí certifikačního orgánu
V Praze dne 15. 01. 2025

Certifikát byl vystaven certifikačním orgánem TAYLLORCOX QCS
TAYLLORCOX s.r.o. Na Florenci 1055/35, 110 00 Staré Město - Praha 1, www.tayllorcox.cz
Kontakt pro ověření platnosti tohoto certifikátu: +420 725 336 797, audit@tayllorcox.com
Member of: TAYLLORCOX UK Ltd., 75 King William St., EC4N, London, United Kingdom

sympulse


03
Cesta ke kvantové odolnosti
sympulse

Cesta ke kvantové odolnosti

Diagnostika

Poznej!

Cíl:
Pochopení kryptografické hrozby a rizik, jejich potlačení či mitigaci.

Vstup:
- Analýza rizik
- Bezpečnostní politiky
- Požadované normy a standardy
- Zmapování účastníků

Výstup:
- Plán projektu
- Školení o kvantové bezpečnosti

1-3 měsíce

Prohledej!

Cíl:
Identifikace, zkoumání a kategorizace kryptografických systémů v IT infrastruktuře.

Vstup:
- IT a síťová architektura
- Bezpečnostní architektura
- Konfigurační databáze
- Existující seznamy kryptografických systémů/aktiv
- Aktivní skenovací nástroje

Výstup:
- Kategorizovaný seznam všech kryptografických aktiv

4-8 měsíců

Roadmapa

Inventarizuj!

Cíl:
Inventarizace používaných kryptografických algoritmů a protokolů a jejich bezpečnostních parametrů

Vstup:
- Pokročilá analýza kryptografických aktiv
- Technické dokumentace
- Rozhovory a workshopy k získání potřebných detailů
- Kontakty třetích stran-dodavatelů

Výstup:
- Kryptografická inventarizace včetně vztahů a návazností a metody mitigace
- Rozdílová analýza

6-9 měsíců

Plánuj!

Cíl:
Vytvoření Migračního plánu ke kvantové odolnosti a komunikace nálezů vedení

Vstup:
- Formální přijetí Migrační plán
- Patch management

Výstup:
- Migrační plán ke kvantové odolnosti
- Analýza trhu s kvantově bezpečnými řešeními
- Migrační management

4-6 měsíců

Migrace a mitigace

Migruj!

Cíl:
Migrace a eliminace rizik jednotlivých aktiv informačních systémů dle Migrační plán

Vstup:
- Migrační plán ke kvantové odolnosti
- Migrační management

Výstup:
- Kvantově-bezpečné informační systémy
- (volitelně) kryptografická agilita

9 měsíců – 3 roky

Co jsou kryptografická aktiva?

Mezi kryptografická aktiva řadíme např.:

- Šifrovací algoritmy
- Kryptografické protokoly
- Šifrovací klíče
- Certifikáty a PKI infrastruktura
- HSM (Hardware Security Modules)
- Šifrovací softwarové knihovny a nástroje
- Digitální podpisy a autentizační mechanismy
- VPN a šifrovací síťové zařízení
- Tokeny pro více faktorovou autentizaci
- Blockchain systémy
- Šifrovací klíče v cloudových prostředích
- Zařízení s integrovanou kryptografii
- Archivovaná kryptografická data
- Systémy pro správu klíčů (KMS)
- A další

sympulse

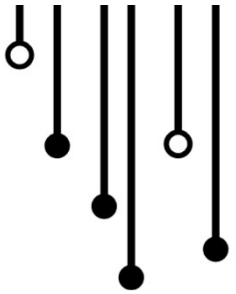
No-regret moves (kroky bez lítosti)

No-regret moves jsou počáteční opatření při přípravě na migraci k postkvantové kryptografii (PQC), která mají smysl a přinášejí hodnotu, i když není jasný časový horizont nebo výsledek vývoje kvantových počítačů.

- **Zmapujte závislosti v dodavatelském řetězci**. Identifikujte závislosti na kryptografii ve vašich IT produktech a slaďte strategie migrace PQC s vašimi dodavateli a dotčenými partnery.
- **Zaveďte správu kryptografických prostředků.** Vytvořte systém pro správu kryptografických aktiv, který zrychlí reakce na incidenty, zlepší kryptografickou flexibilitu a připraví organizaci na hodnocení kvantových rizik.
- **Zrevidujte kryptografické politiky.** Aktualizujte politiky tak, aby odpovídaly současné a očekávané legislativě a zohledňovaly výsledky hodnocení kvantových rizik.
- **Proveďte hodnocení rizik.** Zařaďte kvantové hrozby do řízení rizik, abyste určili optimální čas a strategii migrace na PQC.
- **Odhadněte náklady na migraci.** Vypracujte detailní přehled finančních a kapacitních požadavků na migraci kryptografické infrastruktury pro usnadnění rozhodování.
- **Sledujte regulatorní požadavky.** Monitorujte legislativní změny, abyste sladili strategie s budoucími požadavky a harmonogramy pro nahrazení starších kryptografických standardů.
- **Připravte záložní plán.** Plánujte, jak zajistit kontinuitu podnikání při nečekaných událostech, jako je průlom v kvantových výpočtech nebo útok na stávající kryptografické standardy.
- **Spolupracujte s ostatními.** Sdílejte zkušenosti s jinými organizacemi, zachovávejte interoperabilitu a řešte společné výzvy při migraci na PQC.

sympulse

Jak začít nyní? Pilotem!



- Už jen celková kryptografická inventura může být noční můrou. Samotný přechod ještě větší.
  - Nikdo nemigruje celé systémy ihned. Kde teda začít?
- Doporučovaným přístupem je **vytvořit jeden a více menších pilotních projektů**
  - Můžete jej aplikovat na malé nekritické oblasti.
  - Testují nové post-kvantové algoritmy v reálném prostředí.
  - Identifikují slabá místa v současné kryptografii a infrastruktuře.
  - Snižují rizika migrace díky postupnému zavádění a zpětné vazbě.
  - Zvyšují povědomí a připravenost organizací na budoucí hrozby.
  - A demonstrují schopnosti dodavatele.

sympulse

Kvantová odolnost a bezpečnost od Sympulse

- **Komplexní a praktický přístup:** Sympulse kombinuje dodržování mezinárodních standardů s bohatými zkušenostmi z implementace bezpečnostních řešení v různých prostředích.
- **Služby zahrnují:**
  - Analýzu současného stavu kryptografických aktiv. Návrh bezpečnostních řešení.
  - Postupný přechod na kvantově odolné technologie.
- **Logické celky kryptografických aktiv:** Tento přístup umožňuje efektivnější řízení rizik a snižuje časové i finanční nároky implementace.
  - Zóny, prioritizace aktiv, mapa naléhavosti přechodu na PQC
- **Připravenost na budoucnost:** Sympulse zajišťuje minimalizaci narušení provozu při přechodu na nové technologie a připravenost na kvantové hrozby

Naši klienti

Klienti, u ktorých jsme realizovali řešení v oblasti kybernetické bezpečnosti a detekce rizik.

sympulse

Závěr

- Kvantové počítače přinášejí zásadní bezpečnostní výzvy, které nelze ignorovat.
- Post-kvantové šifrování a kvantová distribuce klíčů jsou klíčové pro ochranu proti kvantovým útokům.
- Sympulse nabízí kompletní řešení od analýzy současného stavu přes migrační plány až po implementaci kvantově odolných systémů.
- Kvantová odolnost je klíčem k ochraně dat v budoucnosti.

Kontakty

❖Kontakty na QSR

- Tomáš Žilavý
  - Sales –T: +420 734 420 317 tomas.zilavy@sympulse.cz
- Michal Křelina
  - Tech Consultant – T: +420 724 094 931 michal.krelina@sympulse.cz
- Marcel Vojtěch
  - Competency Lead – T: +420 724 504 593 marcel.vojtech@sympulse.cz

04

Přílohy

sympulse

Přílohy

- **EU/EC**
  - DOPORUČENÍ KOMISE ze dne 11.4.2024 o plánu pro koordinovanou implementaci přechodu na postkvantovou kryptografii
- **NÚKIB**
  - MINIMÁLNÍ POŽADAVKY NA KRYPTOGRAFICKÉ ALGORITMY - doporučení v oblasti kryptografických prostředků Verze 3.0 (1.7.2023)
  - Příloha - Minimální požadavky na kryptografické algoritmy Verze 1.0
- **Standardizované PQC**
  - FIPS 203 – ML-KEM (CRYSTALS-Kyber)
  - FIPS 204 – ML-DSA (CRYSTALS-Dilithium)
  - FIPS 205 – SLH-DSA (SPHINCS+)
- **Průvodci PQC**
  - TNO - The PQC Migration Handbook, 2nd version 2024
  - Canadian National Quantum-Readiness: BEST PRACTICES AND GUIDELINES
  - ETSI TR 103 619 V1.1.1 - CYBER; Migration strategies and recommendations to Quantum Safe schemes

Děkujeme Vám za pozornost

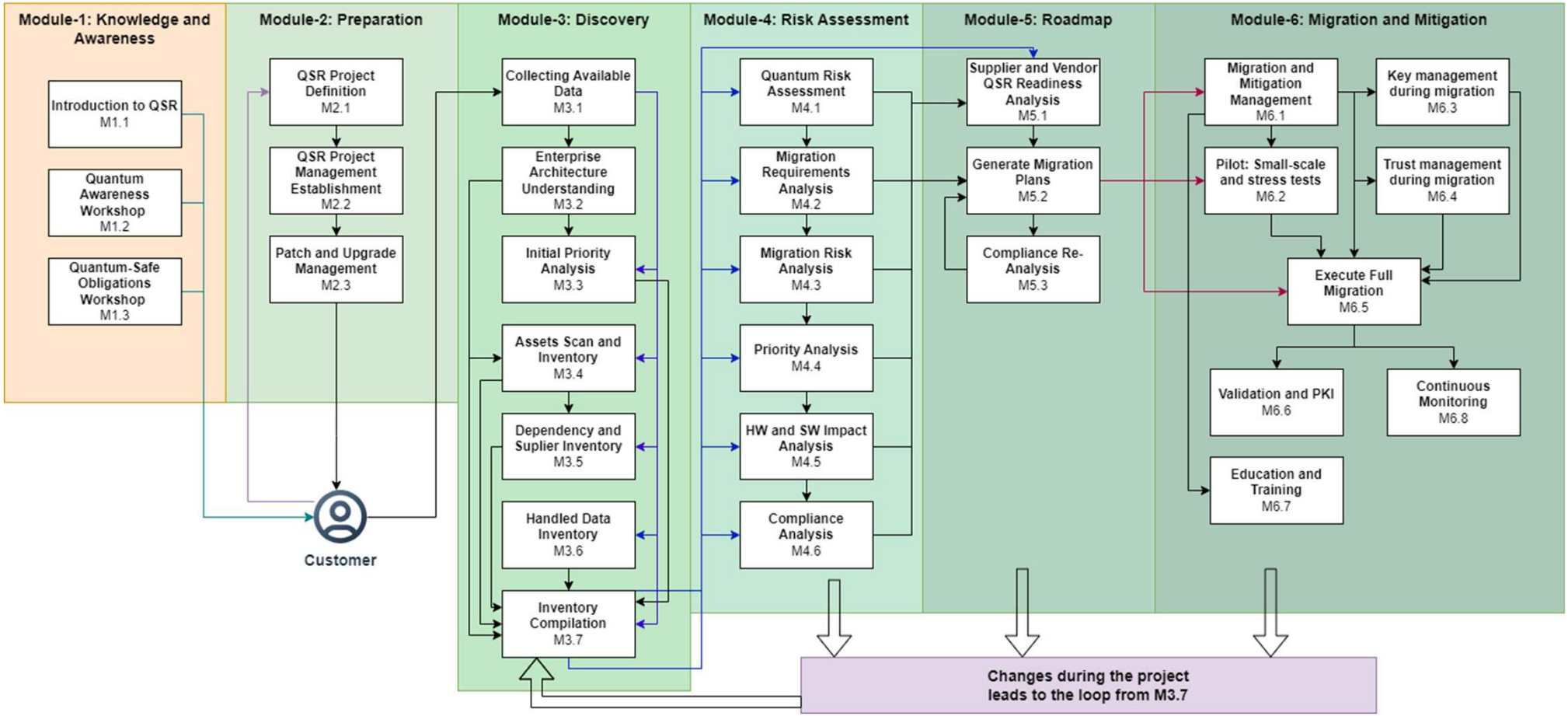
+420 734 420 317

www.sympulse.cz

business@sympulse.cz

Za Brumlovkou 1559/5
140 00 Praha - Michle

QSR Framework Diagram



Procesní kroky ke kvantové odolnosti

- **AS-IS analýza**
  - Založeno na dostupné dokumentaci, architektonickém modelu, CMDB a konzultacích
  - Podpora inventarizace použitím kryptografických inventarizačních nástrojů
  - Klasifikace kritičnosti aplikací
  - Zavedení logických celků kryptografických aktiv
  - Výsledkem je katalog a jedinečný systém pro seskupení kryptografických aktiv

Procesní kroky ke kvantové odolnosti

- **AS-IS analýza**
- **TO-BE analýza, GAP analýza**
  - požadovaného stavu (TO-BE)
  - GAP (rozdílová) analýza AS-IS/TO-BE a doporučení výměny kryptografických algoritmů a protokolů
  - Pro aktiva z GAP analýzy se provede analýza rizik a navrhnou řešení
  - Eliminace rizik např. schování do VPN nebo za firewall
  - Dopadová analýza navrhovaných změn z GAP analýzy
  - Seznam všech kryptografických aktiv a instrukcí k jejich migraci nebo mitigaci

Procesní kroky ke kvantové odolnosti

- **AS-IS analýza**
- **TO-BE analýza, GAP analýza**
- **Migrační plán**
  - Identifikace časové a finanční náročnosti
  - Zmapování potřebných zdrojů a jejich alokace
  - Migrační plán a časový harmonogram
  - Začlenění do rozpočtu a do souladu s ostatními plánovanými projekty

Procesní kroky ke kvantové odolnosti

- **AS-IS analýza**
- **TO-BE analýza, GAP analýza**
- **Migrační plán**
- **Migrace a mitigace rizik**
  - Zahájení kick-off projektu Migrace
  - Řízení migrace dle plánu
  - Konzultace na mitigaci kryptografických algoritmů skrze naše kryptografické experty
  - Testování migračních a mitigačních řešení
  - Projektový reporting
  - Definice a monitoring KPI

sympulse