Zkušenosti s Postquantovou transformací v bance

Matouš Vamberský a Jan Šefčík; Raiffeisenbank

13. – 15. října 2026

ISACA
Czech Republic Chapter

Classification: GENERAL

PQC: zopakování hlavních pojmů

PROČ → ČÍM → CO → JAK

1 HROZBY

Důvěra vytvořená dnes může selhat později.

Q-Day	Kvantová kapacita ohrozí dnešní public-key kryptografii.
HNDL	Harvest Now, Decrypt Later.
TNFL	Trust Now, Forge Later: dnešní podpis může být zneužit v budoucnu.
CRQC	Kryptograficky relevantní kvantový počítač.

2 STANDARDY

Nové algoritmy jsou základ, ne celý program.

ML-KEM	Ustavení klíče • FIPS 203.
ML-DSA	Digitální podpis • FIPS 204.
SLH-DSA	Hash-based podpis • FIPS 205.

3 KRYPTO AKTIVA

Nejdříve musíme vědět, co měníme.

CBOM	Inventář kryptografických závislostí.
PKI/HSM	Trust, certifikáty a ochrana klíčů.
KEM	Mechanismus ustavení klíče.

4 TRANSFORMACE

Cílem je crypto-agility, ne jednorázová výměna.

Agility	Schopnost kryptografii bezpečně měnit.
Hybrid	Klasická + PQC ochrana.
Readiness	Vlastníci, inventář, cílový stav a plán.

PQC není technologický upgrade. Je to řízená změna důvěry napříč bankou.

ISACA Czech Republic Chapter

Classification: GENERAL

Čtyři vrstvy zdrojů mají rozdílnou právní a metodickou váhu

01

LEGISLATIVA

DORA • CRA • GDPR • eIDAS 2 • NIS2

Určuje povinnost řídit rizika, odolnost, dodavatele, produkty a ochranu dat.

02

STANDARDY

NIST FIPS 203 ML-KEM • FIPS 204 ML-DSA • FIPS 205 SLH-DSA

Určují standardizované mechanismy a bezpečné použití.

03

MIGRAČNÍ GUIDANCE

EU Recommendation 2024/1101 • EU Roadmap 2025 • NIST • BSI • ANSSI • ENISA • ETSI

Dává směr, principy a pracovní harmonogram. Není automaticky právně závazná.

04

INTERNÍ ŘÍZENÍ

ISMS • Enterprise Architecture • Risk Management • Procurement • Change Management

Převádí externí rámec do vlastnictví, kontrol, backlogu, KPI a výjimek.

Každá vrstva odpovídá na jinou otázku. Teprve dohromady vytvářejí základ pro řízenou transformaci.

ISACA Czech Republic Chapter

Classification: GENERAL

PQC readiness není compliance status. Je to schopnost řídit změnu.

4 ZDROJE

vytvářejí rámec

- **Legislativa**
- **Standardy**
- **Migrační guidance**
- **Interní řízení**

→

SCHOPNOST BANKY PROVÉST ZMĚNU

01 VLASTNICTVÍ

Strategie, CBOM a kryptografické riziko mají jasné vlastníky.

02 INVENTÁŘ

Banka zná aktiva, závislosti, kontext a kvalitu evidence.

03 ROZHODOVÁNÍ

Priority, výjimky a cílový stav jsou risk-based a auditovatelné.

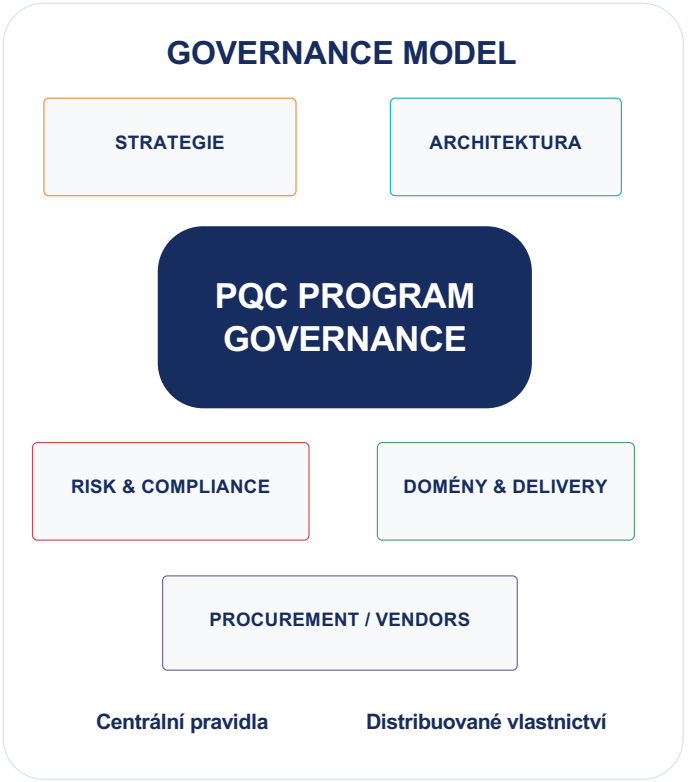
04 REALIZACE

Backlog, financování, delivery a metriky převádějí plán do změny.

ISACA Czech Republic Chapter

Classification: GENERAL

Governance: z kryptografického discovery k řízené migraci



6 otázek k zamyšlení:

1. Kdo vlastní celkovou kryptografickou strategii?
2. Kdo vlastní a validuje informace o kryptografii systémů?
3. Jak se PQC dostane do architektury, projektů a procurementu?
4. Kdo určuje priority a financování migrace?
5. Kdo schvaluje výjimky a akceptaci rizika?
6. **Kdo vlastní CBOM, jeho kvalitu a průběžnou aktualizaci?**

CBOM bez vlastníka je pouze snapshot. Governance z něj musí udělat živý rozhodovací nástroj.

ISACA Czech Republic Chapter

Classification: GENERAL

FROM ZERO TO HERO: CREATING OUR CBOM

BUILDING A COMPREHENSIVE CRYPTO BILL OF MATERIALS CATALOGUE | OUR CRYPTO AGILITY JOURNEY



Start

ZERO

STARTING FROM NOTHING:
DISORGANIZED CRYPTO

THE JOURNEY:
PROCESS & CREATION

HERO:

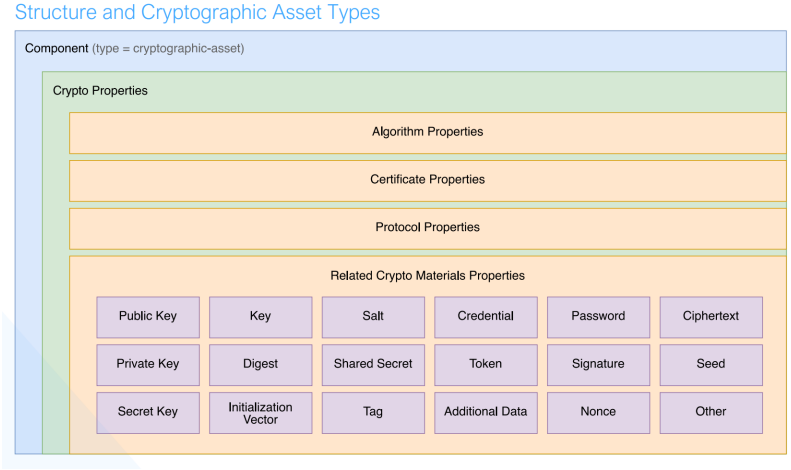
THE CRYPTO CATALOGUE
ARRIVING AT A POLISHED CRYPTO CATALOGUE

End

CBOM – CycloneDX Schema

1. Host
2. Endpoint
3. Protocol
4. Algorithm
5. Certificate
6. Vulnerability

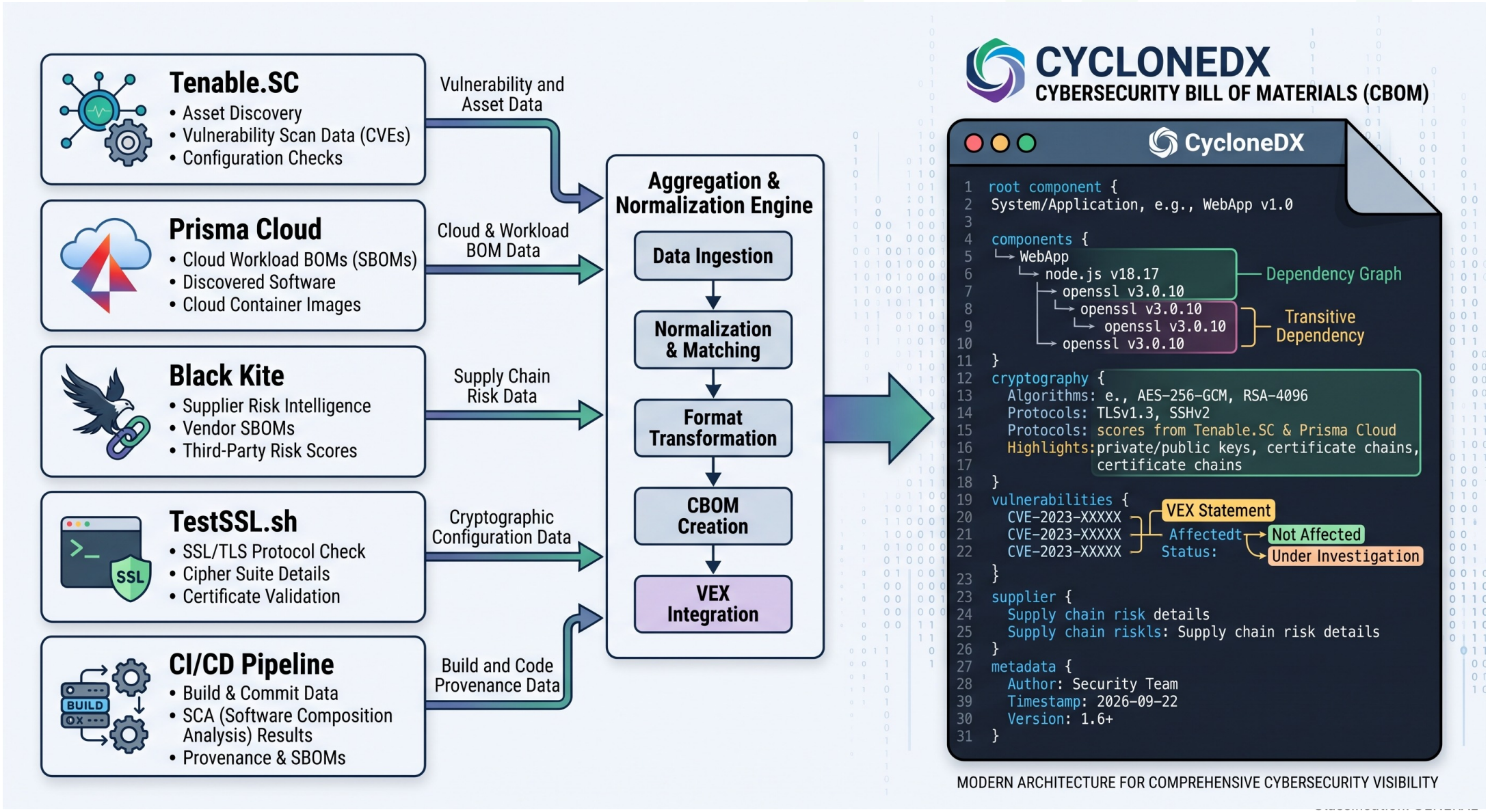
```
CycloneDX 1.7 SBOM (Tenable.sc Export)
├ bomFormat: "CycloneDX"
├ specVersion: "1.7"
├ serialNumber: "urn:uuid:8b3c9281-9b12-42a9-b82b-0e2417e6e5f1"
├ version: 1
|
├ components (The Infrastructure Inventory)
| └ host-10.237.91.6 (Device)
|    ├ name: "server-db-a0"
|    ├ description: "Server"
|    ├ externalReferences (CMDB)
|    | └ https://jira.mycompany.com/jira/secure/insight/assets/ITSM-11464551
|    └ properties
|       └ tenable.sc:host:os: "Linux Kernel 4.18.0-553.144.1.el8_10.x86_64 on Red Hat Enterprise Linux release 8.10 (Ootpa)"
|
├ services (The Open Ports / Sockets)
| └ endpoint-10.237.91.7-8443
|    ├ name: "TLS"
|    └ endpoints: ["https://10.237.91.7:8443"]
|
├ dependencies (The Relationship Graph)
| ├ host-10.237.91.7
| | └ provides ──> [ "endpoint-10.237.91.7-443" ]
|
└ vulnerabilities (The Scan Findings)
  └ vulnerability-104743-10.237.91.7-443
     ├ id: "104743"
     ├ source: { "name": "Tenable.sc" }
     ├ description: "TLS Version 1.1 Deprecated Protocol"
     ├ firstSeen: "2025-11-01T08:00:00Z"
     ├ lastSeen: "2026-09-15T12:00:00Z"
     ├ properties
     | └ tenable.sc:plugin:name: "TLS Version 1.1 Deprecated Protocol"
     ├ detail: "TLSv1.1 is enabled and the server supports at least one cipher."
     └ affects
        └ ref: "endpoint-10.237.91.7-443"
```



https://cyclonedx.org/specification/overview/

ISACA Czech Republic Chapter

Classification: GENERAL


Tenable.SC
• Asset Discovery
• Vulnerability Scan Data (CVEs)
• Configuration Checks
Vulnerability and Asset Data
Prisma Cloud
• Cloud Workload BOMs (SBOMs)
• Discovered Software
• Cloud Container Images
Cloud & Workload BOM Data
Black Kite
• Supplier Risk Intelligence
• Vendor SBOMs
• Third-Party Risk Scores
Supply Chain Risk Data
TestSSL.sh
• SSL/TLS Protocol Check
• Cipher Suite Details
• Certificate Validation
Cryptographic Configuration Data
CI/CD Pipeline
• Build & Commit Data
• SCA (Software Composition Analysis) Results
• Provenance & SBOMs
Build and Code Provenance Data
Aggregation & Normalization Engine
Data Ingestion
Normalization & Matching
Format Transformation
CBOM Creation
VEX Integration
CYCLONEDX
CYBERSECURITY BILL OF MATERIALS (CBOM)
CycloneDX
root component {
System/Application, e.g., WebApp v1.0
components {
WebApp
node.js v18.17
openssl v3.0.10
openssl v3.0.10
openssl v3.0.10
openssl v3.0.10
Dependency Graph
Transitive Dependency
}
cryptography {
Algorithms: e., AES-256-GCM, RSA-4096
Protocols: TLSv1.3, SSHv2
Protocols: scores from Tenable.SC & Prisma Cloud
Highlights:private/public keys, certificate chains,
certificate chains
}
vulnerabilities {
CVE-2023-XXXXX
CVE-2023-XXXXX
CVE-2023-XXXXX
VEX Statement
Affectedt
Status:
Not Affected
Under Investigation
}
supplier {
Supply chain risk details
Supply chain riskls: Supply chain risk details
}
metadata {
Author: Security Team
Timestamp: 2026-09-22
Version: 1.6+
}
MODERN ARCHITECTURE FOR COMPREHENSIVE CYBERSECURITY VISIBILITY

Priority PQC migrace: rozhoduje riziko

NALÉHAVOST MIGRACE = **EXPOZICE** + **DOBA OCHRANY DAT** + **DOBA POTŘEBNÁ KE ZMĚNĚ**

1

EXPOZICE

Jak snadno mohou být data zachycena nebo kompromitována?

- veřejný internet
- příchozí i odchozí spojení
- pásky, disky a IT provoz
- třetí strany a interní hrozby

2

RETENCE A ŽIVOTNOST DAT

Jak dlouho musí data zůstat důvěrná?

- „shelf-life“ šifrovaných dat
- jde o dlouhodobě citlivá data?
- primárně “Data at rest”
- HNDL posouvá riziko do současnosti

Začněte tam, kde se kombinuje vysoká expozice, dlouhá životnost dat a dlouhá doba změny.

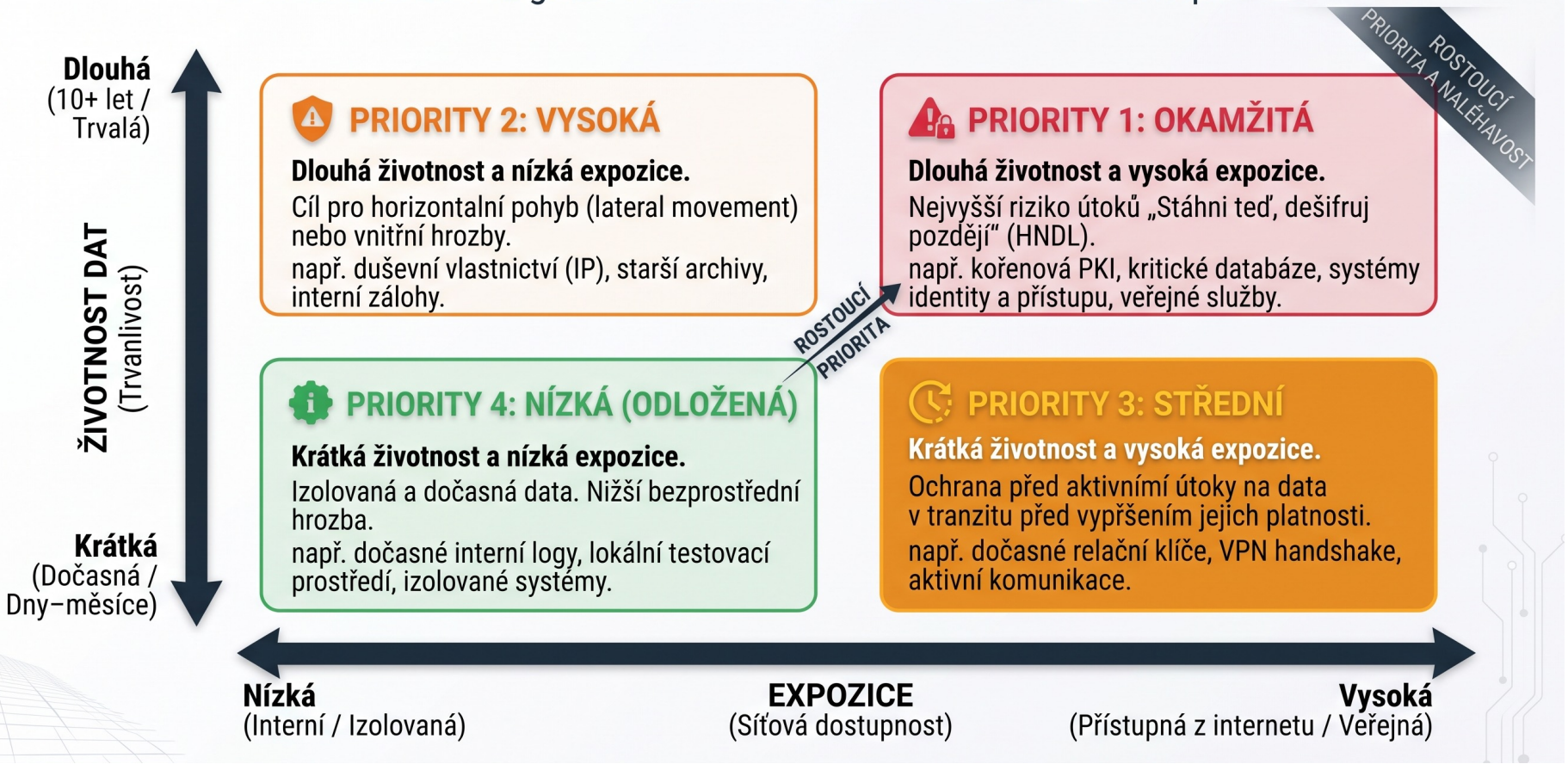
ACT NOW | PLAN NEXT | MONITOR & PREPARE

ISACA Czech Republic Chapter

Classification: GENERAL

MATICE PRIORIT MIGRACE NA PQC

Určení naléhavosti migrace na základě životnosti dat a síťové expozice.



ISACA Czech Republic Chapter

Classification: GENERAL

PQC migrační roadmapa: prioritizovaná matice

PRIORITA	ARCHITEKTONICKÁ VRSTVA	KLÍČOVÝ ROZSAH	TYPICKÝ MIGRAČNÍ VZOR	PŘÍKLAD CÍLOVÉHO OBDOBÍ
1	**Externí perimetr a veřejný vstup**	Veřejné mobilní/webové API, edge load balancery, WAF, externí API gateway	Nativní upgrade / proxy na perimetru	**Q1 2027 – Q4 2027**
2	**Vyhrazené linky třetích stran a B2B**	EDI a B2B gateway, SWIFT, clearingové linky, IPsec/MACsec VPN, dedikované linky	Nativní upgrade / hybridní IPsec	**Q3 2027 – Q2 2028**
3	**Tier 1 infrastruktura a Tier 1 aplikace**	Kritické aplikace, integrační platformy, middleware, PKI, IAM, orchestrace, messaging, SDLC/CI/CD	Nativní upgrade / refaktoring / SDK upgrade / síťová izolace	**Q1 2028 – Q4 2028**
4	**Tier 2 infrastruktura a Tier 2 aplikace**	Interní API a MQ gateway, datové sklady, CRM, ERP, COTS	Service mesh proxy / produkční vendor patche	**Q1 2029 – Q4 2029**
5	**Tier 3, legacy a EOL systémy**	Systémy k vyřazení, krátká retence dat, intranet, telemetrie, observabilita	Akceptace rizika / síťová izolace / vyřazení	**+ 2030**

Roadmapa není kalendář výměny algoritmů. Je to řízené pořadí rozhodnutí a závislostí.

ISACA Czech Republic Chapter
Classification: GENERAL

Kryptografické migrační vzorce – směrem ke crypto-agility

1 Změna konfigurace / parametrů

TLS 1.3 + Groups Extensions, konfigurace OpenSSH, konfigurace API gateway

RYCHLÁ ZMĚNA

2 Aktualizace knihoven

Upgrade BouncyCastle/OpenSSL, migrace na SDK připravená na PQC

OPAKOVATELNÉ

3 Migrace / refaktoring

Upgrade databáze, upgrade COTS, migrace PKI, vynucení hybridních klíčů

HLUBŠÍ ZÁSAH

4 Závislost na dodavateli

Legacy aplikace, nepodporovaná integrační platforma

EXTERNÍ ZÁVISLOST

5 Síťová izolace

Reverse proxy, virtuální patching

RISK TREATMENT

Výsledek: méně unikátních projektů, více standardních migračních patterns.

ISACA Czech Republic Chapter
Classification: GENERAL

Lessons learned: nejdříve inventář aka CBOM, potom akce

1 WORKSHOPY

Pochopit data v klidu i při přenosu

2 KONTEXT

EA, risk modely, interní wiki

3 SKENOVÁNÍ

Potvrdit realitu „pod kapotou“

4 NORMALIZACE

Omezit duplicity a šum

5 AUTOMATIZACE

Zapojit do vulnerability managementu

Zdroje automatizovaného discovery

ON-PREMISE

Qualys VMDR • Rapid7 Nexpose • Tenable.SC • nmap • Wireshark • IBM Guardium Quantum Safe

CLOUD

Wiz • Palo Alto Networks Prisma Cloud • CrowdStrike Falcon Cloud Security

PERIMETR

nmap • TestSSL.sh

Pozor: horizontální skenovací nástroje samy o sobě generují velké množství šumu.

Automatizujte a udělejte proces opakovatelný.

ISACA Czech Republic Chapter

Classification: GENERAL

Lessons learned: začněte na perimetru

PŘÍCHOZÍ SPOJENÍ

Cloudflare TLS 1.3 s hybridní výměnou klíčů

AWS CloudFront, AWS API Gateway

Azure Front Door, Azure CDN, Azure API Management

Kubernetes Router

VIDITELNÁ EXPOZICE

ODCHOZÍ SPOJENÍ

Složitější oblast: spojení jsou iniciována zevnitř a nelze je snadno skenovat.

Kubernetes Pods

AWS EC2, Azure VM

AWS Lambda, Azure Functions

SLEPÉ MÍSTO

ISACA Czech Republic Chapter

Classification: GENERAL

#SafebyRaiffeisen project





Co-funded by the European Union
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them

Supported by ECCC
The project funded under Grant Agreement No. 101158662 is supported by the European Cybersecurity Competence Centre

ISACA Czech Republic Chapter

Classification: GENERAL

ISACA
Czech Republic Chapter