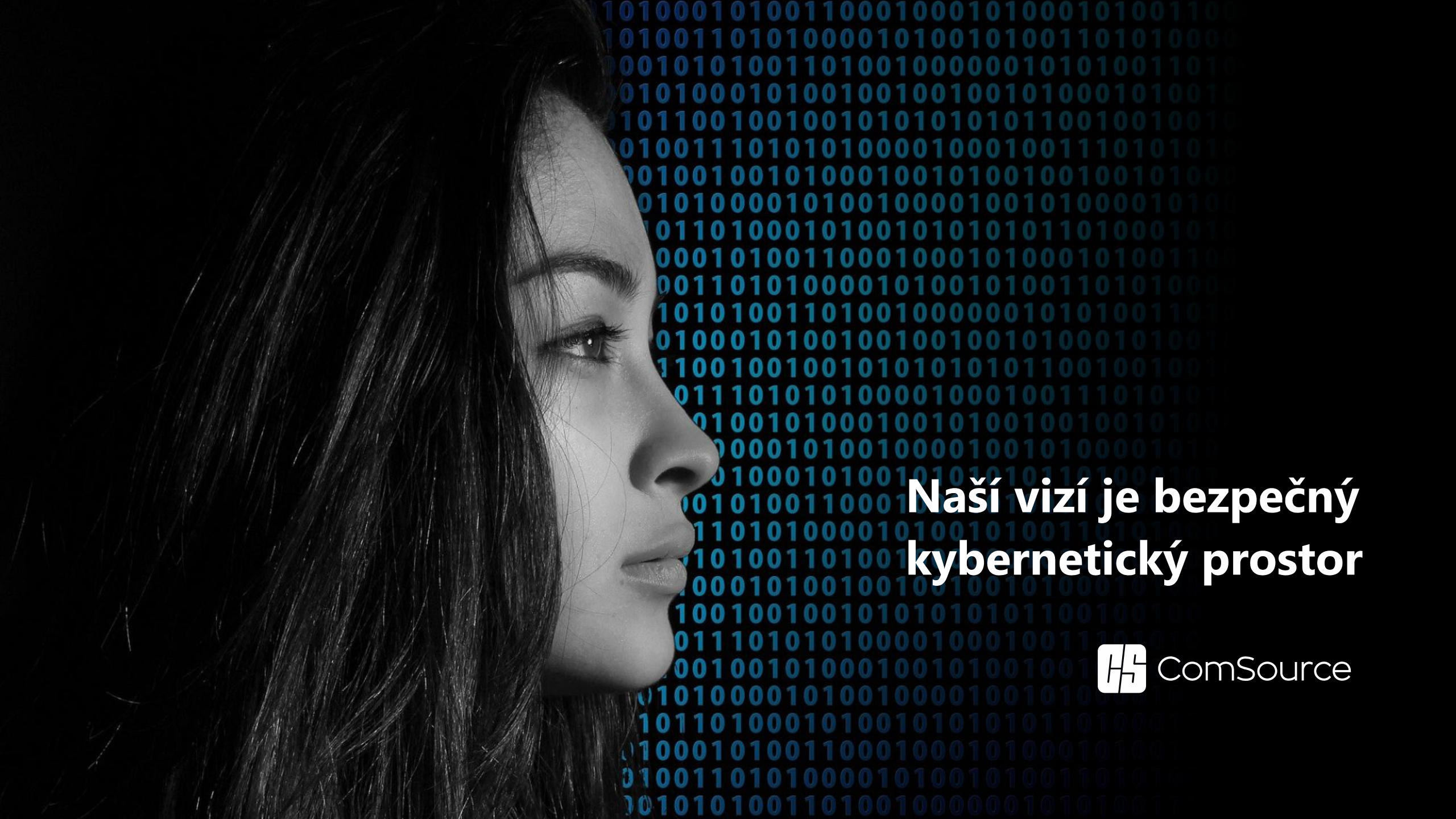
ComSource

# Hrozba v podobě kvantových počítačů? Ano, ale co dál?

Prezentuje: Marek Kocan, Lukáš Krajíček



# Naší vizí je bezpečný kybernetický prostor

ComSource

# ComSource

- Specializace na několik pečlivě vybraných vendorů.

# ComSource partnerství

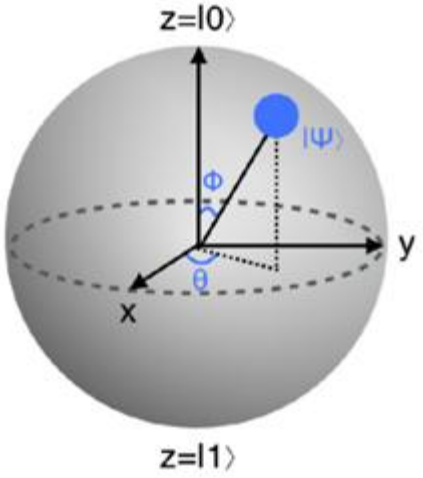
Jsme součástí týmu CSIRT (Computer Security Incident Response Team). Úkolem národního týmu CSIRT.CZ je ve spolupráci s Národním bezpečnostním úřadem reagovat, koordinovat a řešit bezpečnostní incidenty v oblasti bezpečnosti IT.

ComSource je aktivním členem české pobočky AFCEA (Armed Forces Communication and Electronics Association). Členství v této mezinárodní organizaci nám umožňuje sdílet a rozvíjet naše know-how v oblasti kybernetické bezpečnosti a ICT technologií.

ComSource je členem projektu FENIX, který vznikl v roce 2013 na půdě českého peeringového uzlu, sdružení NIX.CZ, jako reakce na intenzivní DDoS útoky, kterým toho roku čelila významná česká média, banky nebo operátoři.

# Je to tu ...

# Rychlé opáčko



*qubit*

- Nejde o nuly a jedničky, ale o (kvantovou) superpozici těchto dvou stavů
- Neřešitelné pomocí nul a jedniček se stane řešitelným (v rozumném čase a za rozumných nákladů)
- Současná reprezentace (až) všech 2^n možných stavů
- Qubity tedy mohou být ve více stavech současně a kvantové počítače tak mohou pracovat skutečně paralelně (exponenciální paralelismus)
- Speciální algoritmy – Groverův (vyhledávání v nestrukturovaných datech), Shorův (faktorizace velkých čísel na prvočísla) …
- Postkvantová a kvantová kryptografie

# Proč je to špatně aneb např. Shorův algoritmus

- Peter Williston Shor 1994
- Jeden z neznámějších kvantových algoritmů
- Efektivní faktorizace velkých čísel aneb hledání součinu prvočísel
- Polynomiální náročnost (základ log N) vs. exponenciální (základ $e^N$)
- Prvočísla jako jeden z klíčových základů moderní kryptografie
- Podstata hledání periodické struktury (periodu funkce $a^x \bmod N$)
- 21 – z hlavy víme, že je to 3 * 7
- Zvolíme číslo a menší než N, musí být nesoudělná: gcd(a,N) = 1
  - např. a = 2; gcd(2,21) = 1
  - ** gcd = Greatest Common Divisor*

# Shorův algoritmus

- Hledáme periodu funkce $a^x \bmod N$

$$2^1 = 2 \mod 21 = 2$$

$$2^2 = 4 \mod 21 = 4$$

$$2^3 = 8 \mod 21 = 8$$

$$2^4 = 16 \mod 21 = 16$$

$$2^5 = 32 \mod 21 = 11$$

$$2^6 = 64 \mod 21 = 1 \checkmark$$

- Perioda je tedy 6, sudé číslo OK (liché obvykle volíme jiné)
- Budeme počítat $gcd(a^{r/2} \pm 1, N)$
  - gcd(8 + 1,21) = gcd(9,21) = 3
  - gcd(8 - 1,21) = gcd(7,21) = 7
- A máme faktory 3 a 7 (kontrola: ano, je to 21☺ )
- Pro hledání periody se využije kvantová Fourierova transformace

# Náročnost prolomení šifrování

- Prvočíselný rozklad základem *některých* šifrovacích metod (RSA)
  - → Náročnost rozkladu není ekvivalent *náročnosti prolomení šifrování* (buzzword)
  - → Jako příklad postačí; efektivní rozklad představuje významné ohrožení

## Náročnost (klasické algoritmy)

RSA Factoring Challenge (1991)
- **RSA-2048** *(4,168M kč)*

→ Lenstra elliptic-curve factorization
- Geometrie*!*
- 50-60 cifer (neefektivní pro malá čísla)

$$2,73^X \quad \text{pro} \quad X = C\sqrt{\ln(P)\ln(\ln(P))}$$

→ General number field sieve
- Algebraická hra s čísly
- Nad 100 cifer

$$2,73^X \quad \text{pro} \quad X = C\sqrt[3]{\ln(N)}\sqrt[3]{\ln(\ln(N))^2}$$

## Náročnost (kvantové algoritmy)

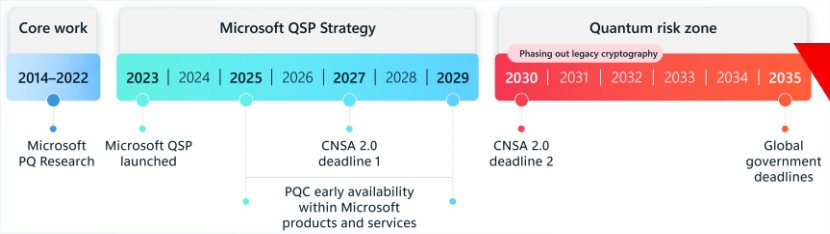
→ Shorův algoritmus (teoreticky)

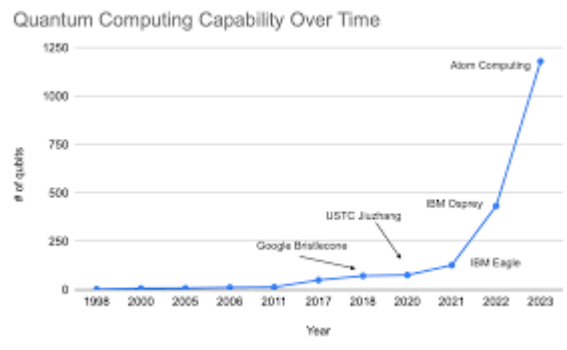
$$\ln(N)^3$$

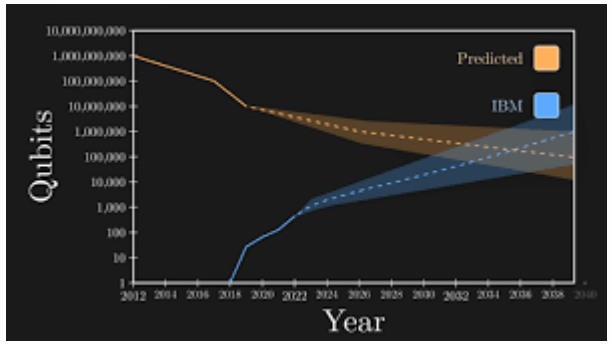
Počet qubitů k rozlomení RSA 2048 pod 8 hodin: **20 milionů "noisy" qubitů**

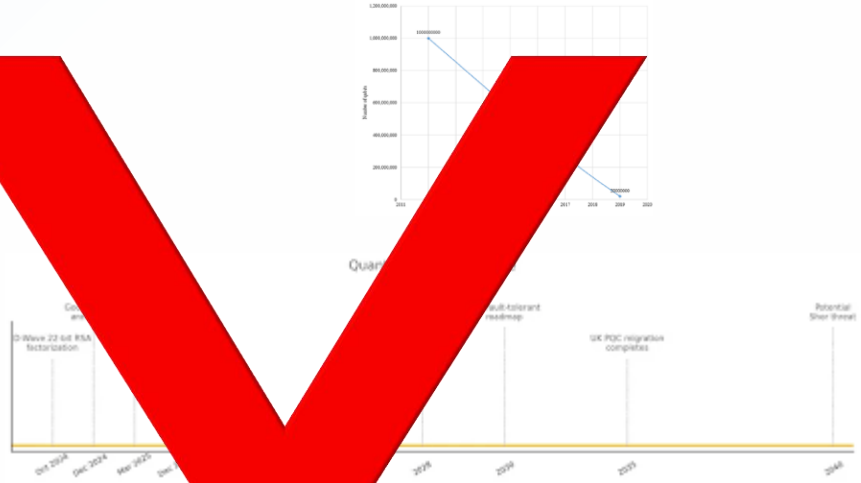
[arXiv 1905.09749] Gidney-Ekerå, 13. 4. 2021
How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits

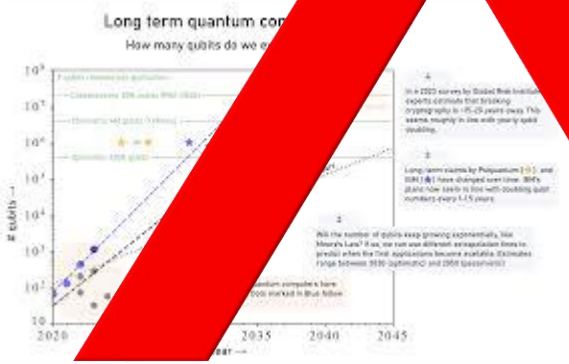
# Predikce, predikce, predikce …

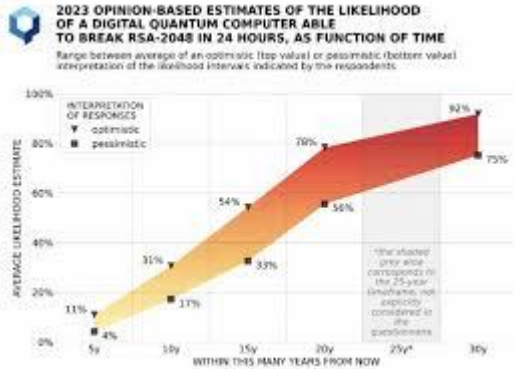


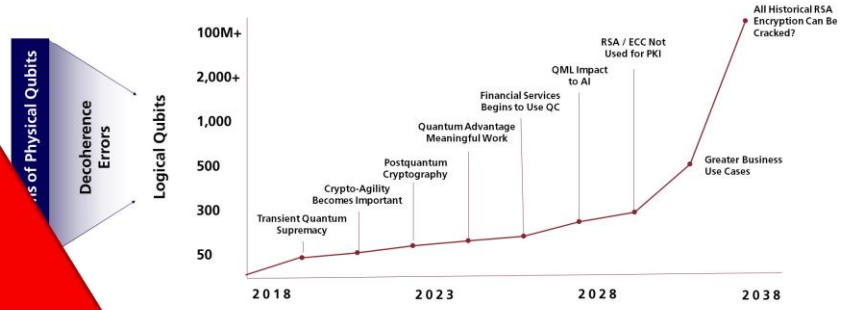






PQC uses a new set Quantum Resistant Algorithms, created by researchers and tested by industry standard bodies such as NIST and ANSSI that are in the process of becoming a part of compliance requirements.




Source: Kumar M, "Post-quantum cryptography Algorithm's standardization and performance analysis"

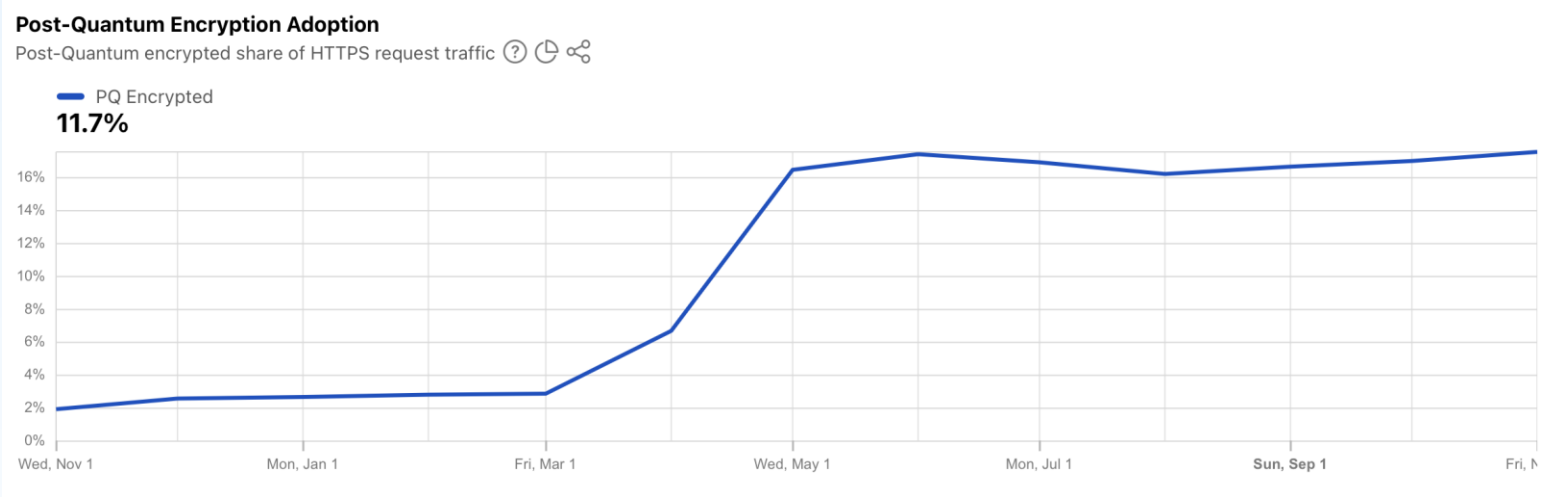
# Postkvantová kryptografie

- Kryptografie odolná vůči útokům pomocí kvantových počítačů (pozor: Harvest now, decrypt later)
- Využití tradičních počítačů a lepších algoritmů
- Standardy NIST (jsou zdarma i pro komerční užití):
  - Úsilí od začátku druhé poloviny minulé dekády
  - 8/2024: FIPS 203 - Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM)
  - 8/2024: FIPS 204 - Module-Lattice-Based Digital Signature Standard (ML-DSA)
  - 8/2024: FIPS 205 - Stateless Hash-Based Digital Signature Standard (SLH-DSA)
  - FN-DSA - FFT over NTRU lattices Digital Signature Standard
  - HQC - Hamming Quasi-Cyclic (2027?)
- EK: Doporučení pro koordinovanou implementaci přechodu na PQC (4/2024)

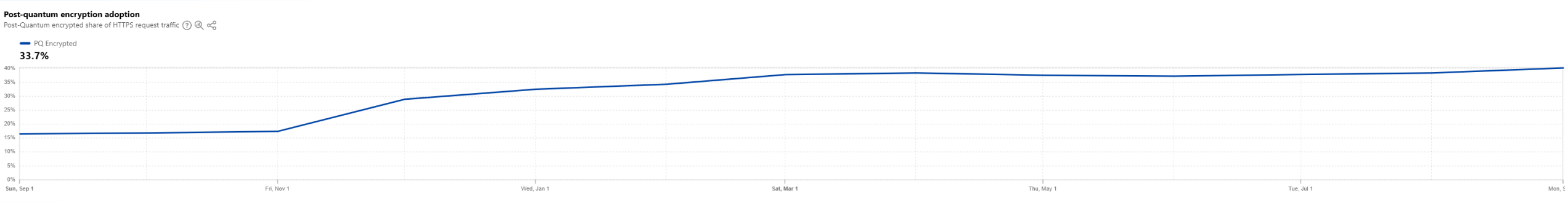
# Míra přijetí ve světě

- Nad rámec pokusů odhady uvádí desítky až vyšší stovky řešení s implementovanou podporou PQC
- Operační systémy, aplikace, knihovny, hardware i služby:
  - Apple iOS, MS SymCrypt / SymCrypt-OpenSSL, iMessage, Google Chrome, Mozilla Firefox, AWS KMS, Cloudflare SWG, Java 24, Infineon PSOC (MCU), SEALSQ, Juniper JUNOS, Cisco, F5 ADSP, Facebook, Chainguard, Thales Luna HSM, Futurex, QuSecure (IoT, OT, space), Quantum Xchange …
- Odhad adopce cca 30 procent v roce 2030, cca 80 procent v roce 2035
- Trh cca 8 miliard USD 2030 / cca 12 miliard 2035

# Cloudflare Radar 2023 až 2025



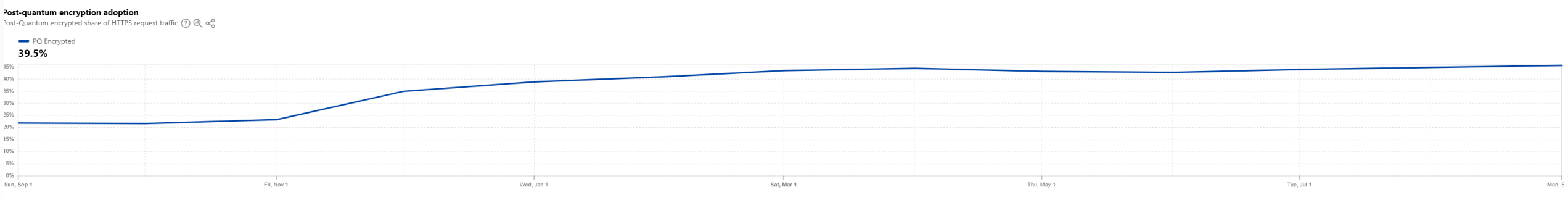

2->16->40




ComSource

# Česká republika?

- https://nukib.gov.cz/cs/infoservis/aktuality/2156-portal-nukib-nove-podporuje-kvantove-odolnou-kryptografii/
- Projekt NESPOQ (strategický výzkum pro PQC/QKD)
- Monet+ (platební systémy)
- Akademická sféra (do FPGA, ESP32 …)
- A co banky – přeneseně z jiných předpisů musí, ale naše zkušenosti mj. zahrnují My to teď nepotřebujeme, To je moc daleko a Dodavatelé z oblasti postkvantové kryptografie nám sami řekli, že času máme dost



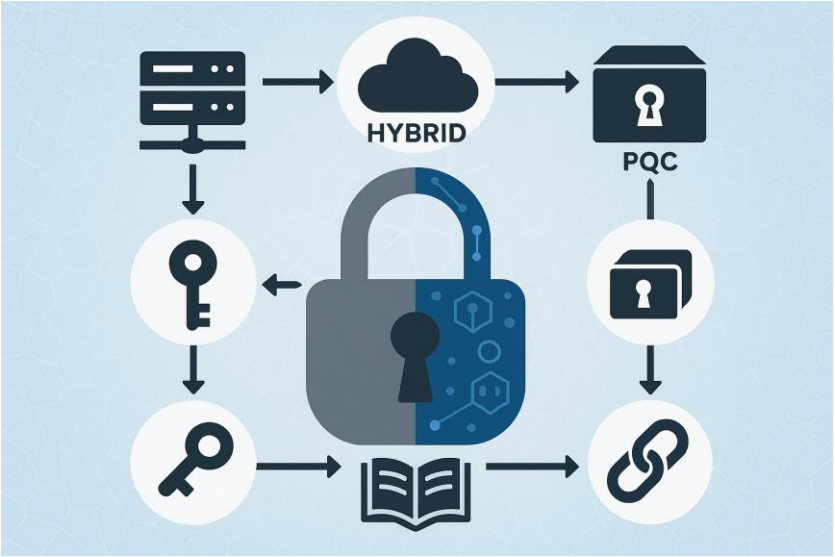
# Bez právního pohledu to nejde …

- Součástí rozsahu řízení kybernetické bezpečnosti jsou aktiva související s poskytováním regulované služby.
- Bezpečnostními opatřeními jsou organizační a technická opatření, jejichž účelem je zajištění řádného poskytování regulované služby a kybernetické bezpečnosti aktiv.
- Poskytovatel regulované služby je povinen v rámci stanoveného rozsahu zavádět a provádět bezpečnostní opatření v míře nezbytné pro zajištění kybernetické bezpečnosti regulované služby.
- Pro poskytovatele regulované služby v režimu vyšších povinností jsou … technickými opatřeními … kryptografické algoritmy.
- … používá pouze aktuálně odolné kryptografické algoritmy …
- … zajistí pomocí aktuálně odolných kryptografických algoritmů …
- … zohledňuje doporučení a metodiky v oblasti kryptografických algoritmů vydané Národním úřadem pro kybernetickou a informační bezpečnost. …
- Finanční subjekty navrhují, opatřují a uplatňují politiky, postupy, protokoly a nástroje v oblasti bezpečnosti IKT, jejichž účelem je zajistit odolnost, kontinuitu provozu a dostupnost systémů IKT, zejména těch, které podporují zásadní nebo důležité funkce, a udržet vysoké standardy dostupnosti, hodnověrnosti, integrity a důvěrnosti údajů během jejich uchovávání, používání i přenosu.

# My máme NÚKIB

- NÚKIB: Kvantová hrozba a kvantově odolná kryptografie, příloha dokumentu *Minimální požadavky na kryptografické algoritmy* (2/2025)
  - K4 – Hybridní nebo samostatné použití postkvantové kryptografie?
  - K6 – Výběr kvantově odolné kryptografie
  - K7 – Začlenění postkvantové kryptografie do kryptografických protokolů
- Vysoce prioritní oblasti:
  - Algoritmy pro ustanovení klíčů pro ochranu citlivých informací kritické úrovně důvěrnosti – přechod ke kvantově odolným hybridním kombinacím nebo k samostatným postkvantovým KEM/Encryption je vysoce naléhavý. Jako vhodný termín jeho ukončení NÚKIB odhaduje na konec roku 2030.
  - V oblasti ochrany integrity firmware a software při jejich aktualizacích doporučení začít využívat samostatné kvantově odolné algoritmy LMS a XMSS (*NIST 2020, nevyžadují hybridní přístup*) co nejdříve.
- Doporučená samostatná postkvantová kryptografie
  - LMS a XMSS pro digitální podpisy pro ochranu integrity firmwaru a softwaru
  - ML-KEM-1024 pro ustanovení klíčů
  - ML-DSA-87 pro digitální podpis s obecným použitím
- Kvantová zranitelnost a kvantová odolnost u symetrických šifer
  - Preference blokových šifer před proudovými
  - Všechny šifry s délkami klíčů 128 bitů a 192 bitů jsou kvantově zranitelné
  - Všechny šifry s délkou klíče 256 bitů jsou kvantově odolné

# Vhodná opatření

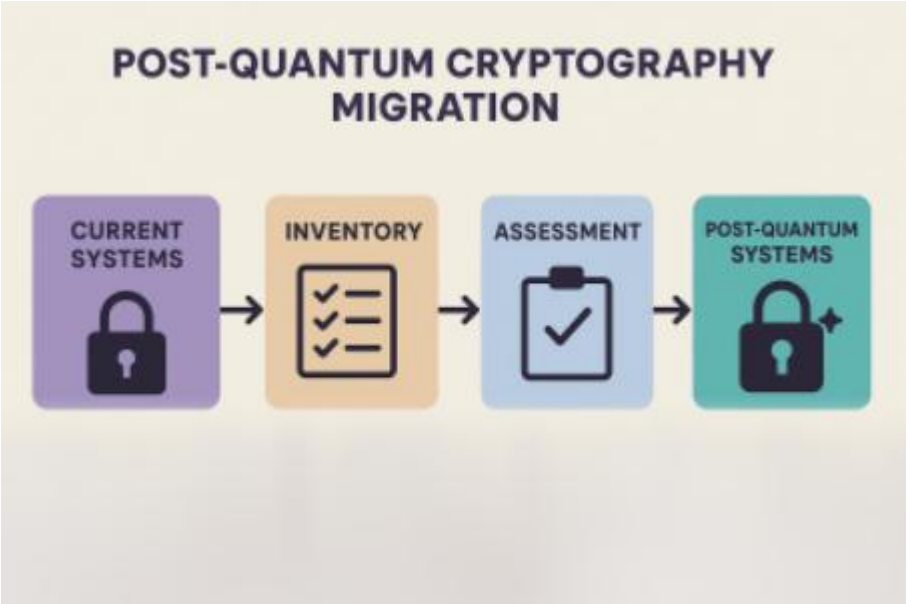



- Pochopení problematiky
- Získání přehledu a stanovení cílů
- Revize kryptografických opatření vč. používaných algoritmů (dodavatelských řešení, knihoven ...)
- Zmapování kryptografických závislostí
- Nasazení vhodných algoritmů (hybridní, PQC)
- Zvážit využití HSM s podporou PQC
- Pouhá změna algoritmů nestačí – je nezbytná komplexní proměna celé provozní a bezpečnostní informační architektury. Od výpočetních prostředků a operačních systémů přes nástroje pro správu klíčů až po podchycení problematiky PQC v celém dodavatelském řetězci aneb holistická transformace.

# Jak to vidí ComSource aneb ochutnávka metodiky

- Úvod do problematiky …
- … stanovení cílů …
- … identifikace a inventarizace …
- … posouzení použitých algoritmů …
- … výběr vhodných algoritmů a doporučení …
- … návazné kroky
  - organizační
  - technické
  - konzultační

*Ucelená metodika bude po ověření představena na přelomu 25/26*



# Kulatý stůl aneb určitě se na nás koukněte

# My nevíme …

# Otázky?

# Děkujeme za pozornost

Email: marek.kocan@comsource.cz lukas.krajicek@comsource.cz

Tel: 604 766 243