



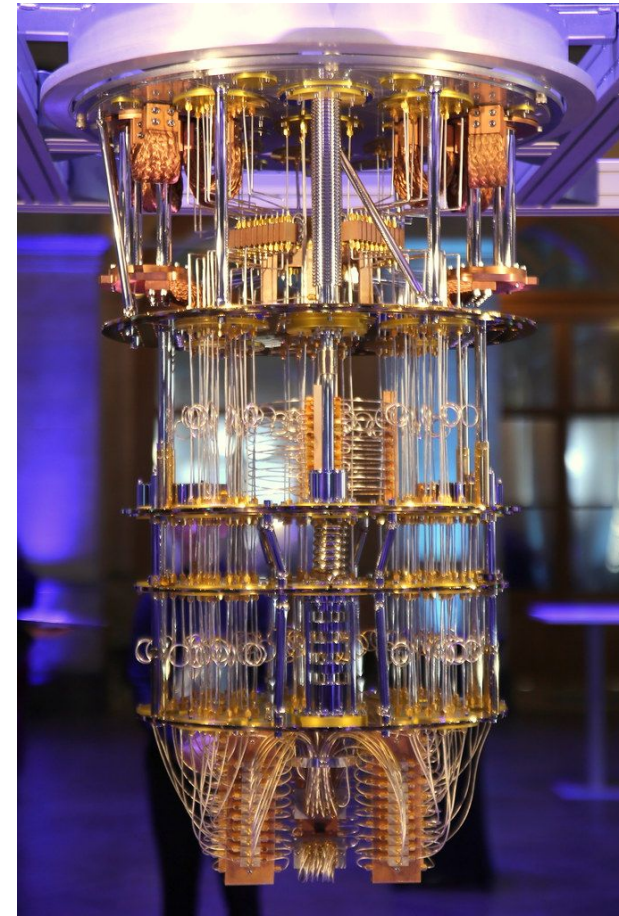
Koho bude zajímat postkvantová kryptografie

Matěj Týč
Engineering Manager

Proč nás toto znervózňuje?

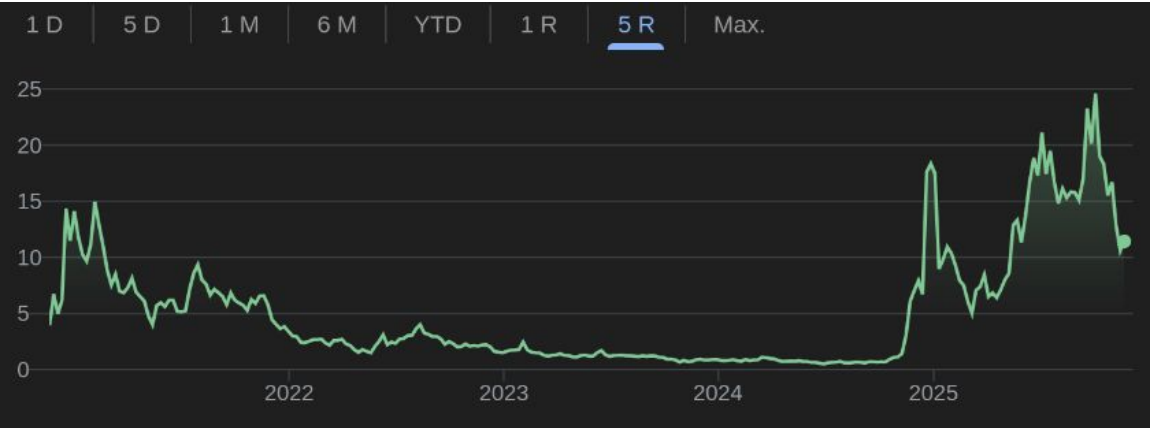
Umí to věci?

- ▶ Extrémně drahé
- ▶ Složité na obsluhu
- ▶ V praxi na nic

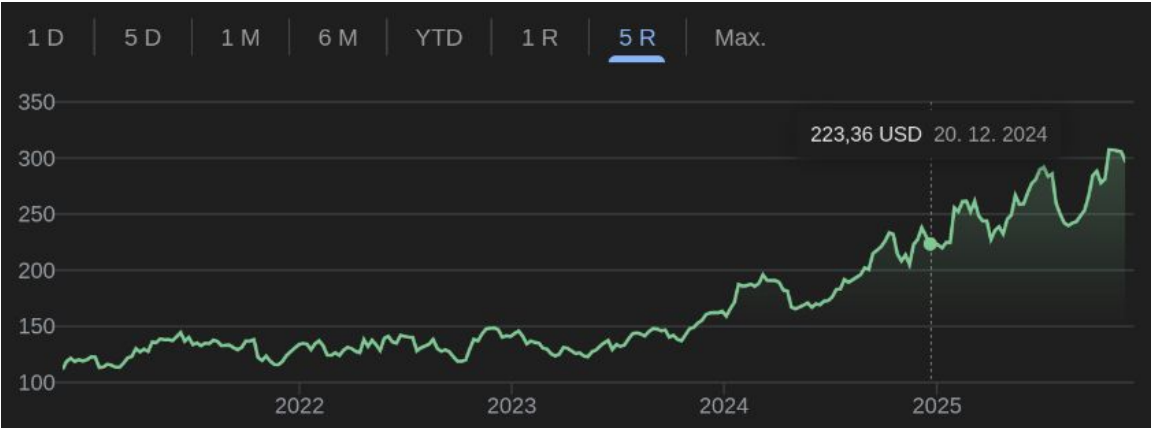


Proč nás toto znervózňuje?

Věří tomu trh?



Quantum Computing Inc.



IBM

Asymetrická kryptografie

Je to zázrak

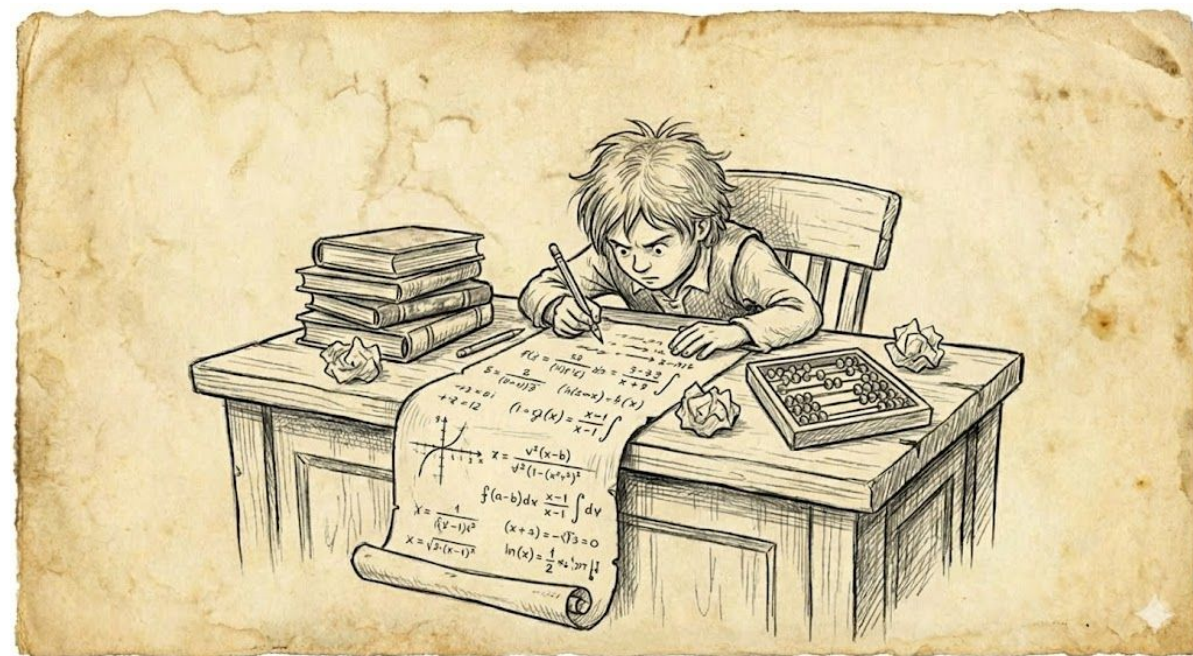
- ▶ Bob i Alice se mohou důvěrně bavit
- ▶ Pokud návod na zašifrování
nestačí k odvození
návodu na rozšifrování



Asymetrická kryptografie

Příklad

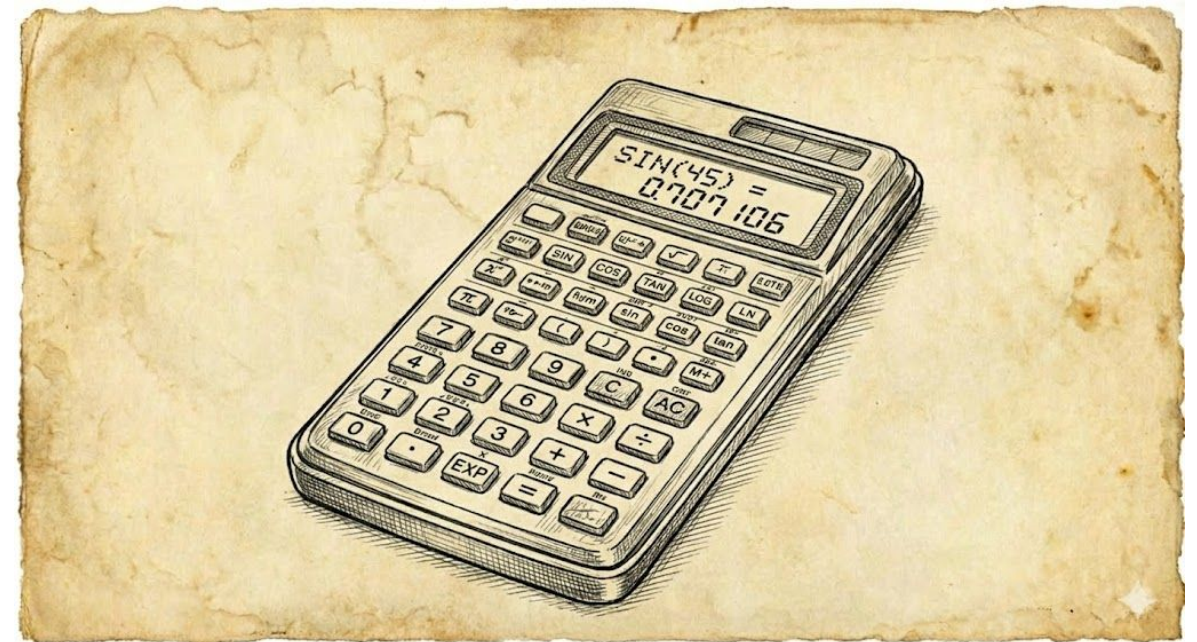
- ▶ $7.87^2 = 61.9369$ – dítě s tužkou a papírem
- ▶ $\sqrt{61.9369} = 7.87$ – pouze s tužkou a papírem
velice obtížné



Asymetrická kryptografie

Příklad

- ▶ $7.87^2 = 61.9369$ – jednoduché
- ▶ $\sqrt{61.9369} = 7.87$ – také jednoduché



Scénáře útoků

Uchování a následné rozšifrování

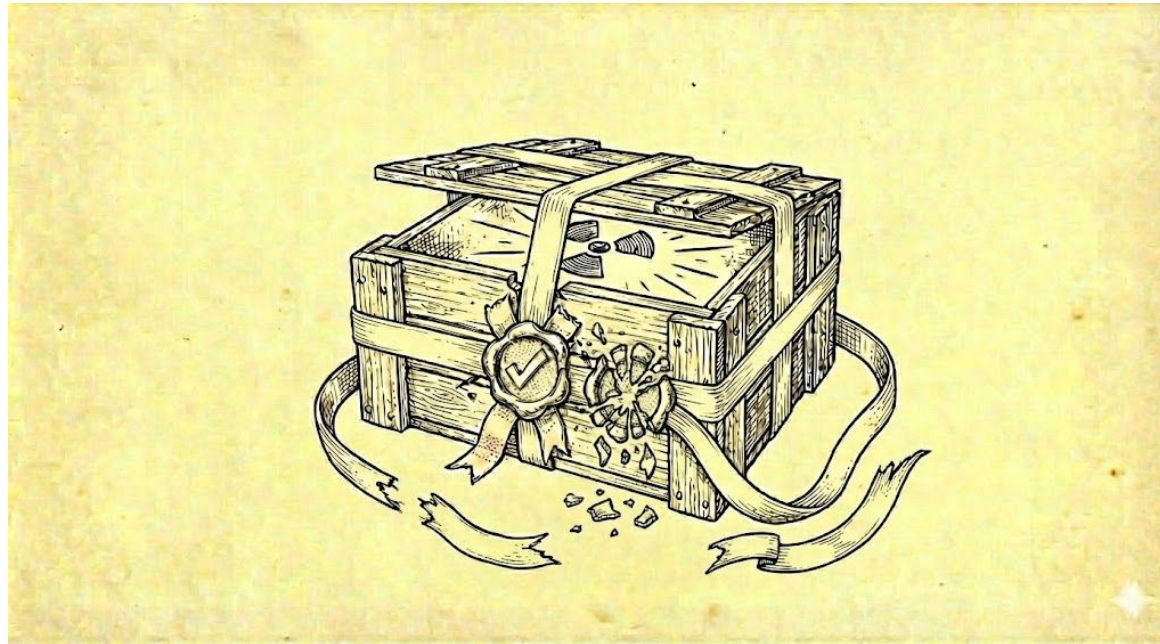
- ▶ Odposlech šifrované komunikace později rozšifrovaný kvantovým počítačem



Scénáře útoků

Podvržení firmwaru

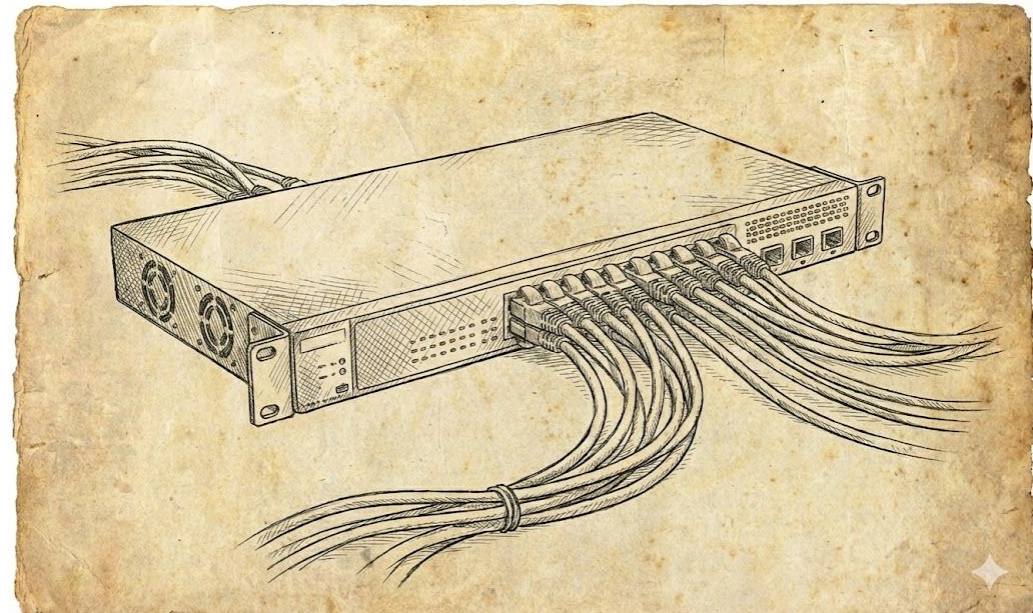
- ▶ Podepsání updatu podpisem podvrženým pomocí kvantového počítače



Protiopatření

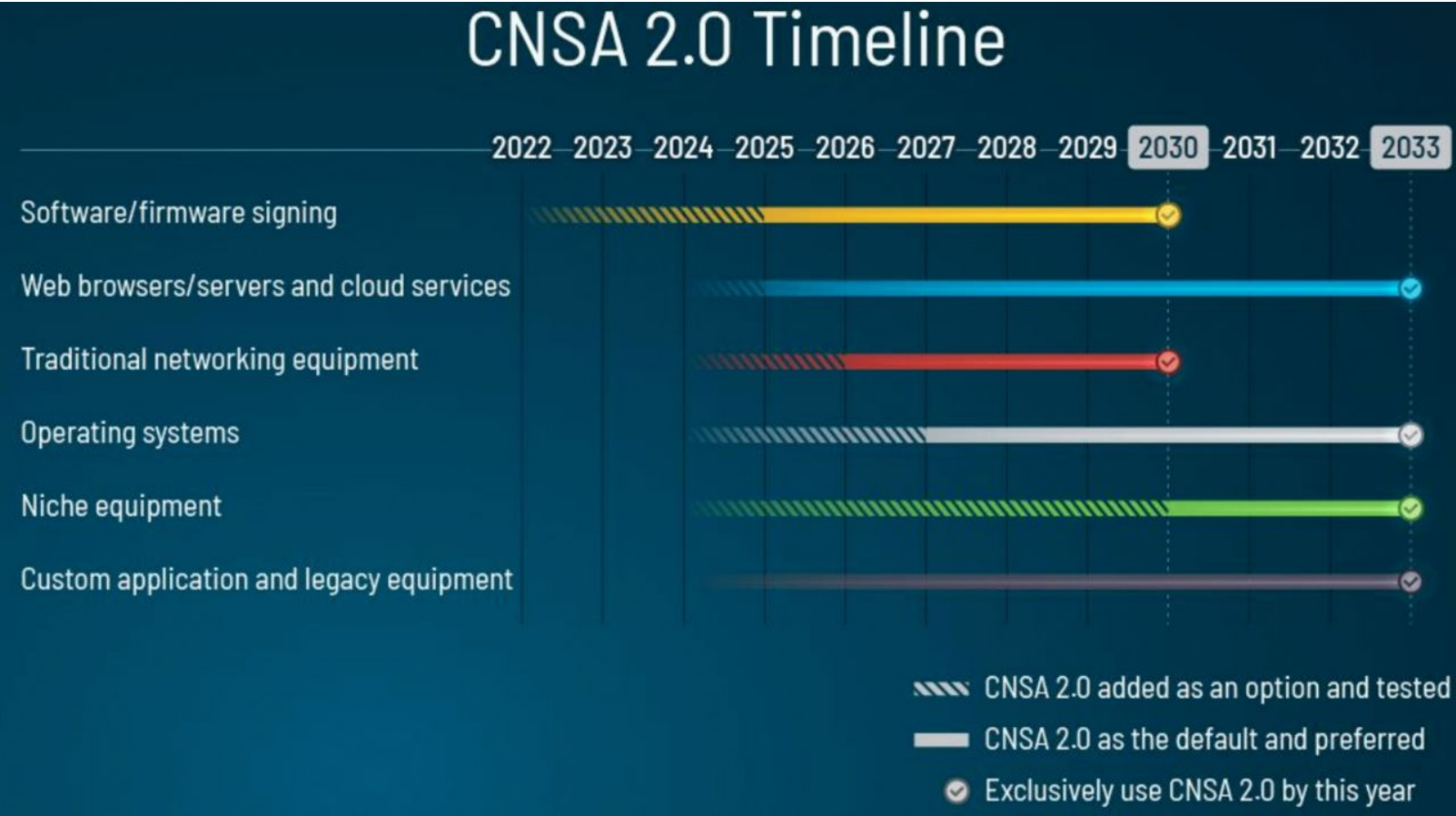
Co ani kvantový počítač nedokáže

- ▶ Složitější algoritmy
 - CPU: Stejná náročnost
 - Paměť: 5x nárůst, OK
 - Síť: 5–10 nárůst dat, problém



Svět již jedná

USA velice pospíchají



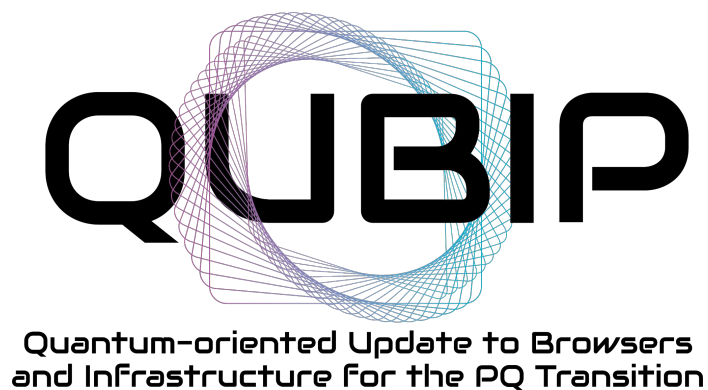
Svět již jedná

EU je opatrnější

A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography

Part 1, Version: 1.1, EU PQC Workstream

11.06.2025



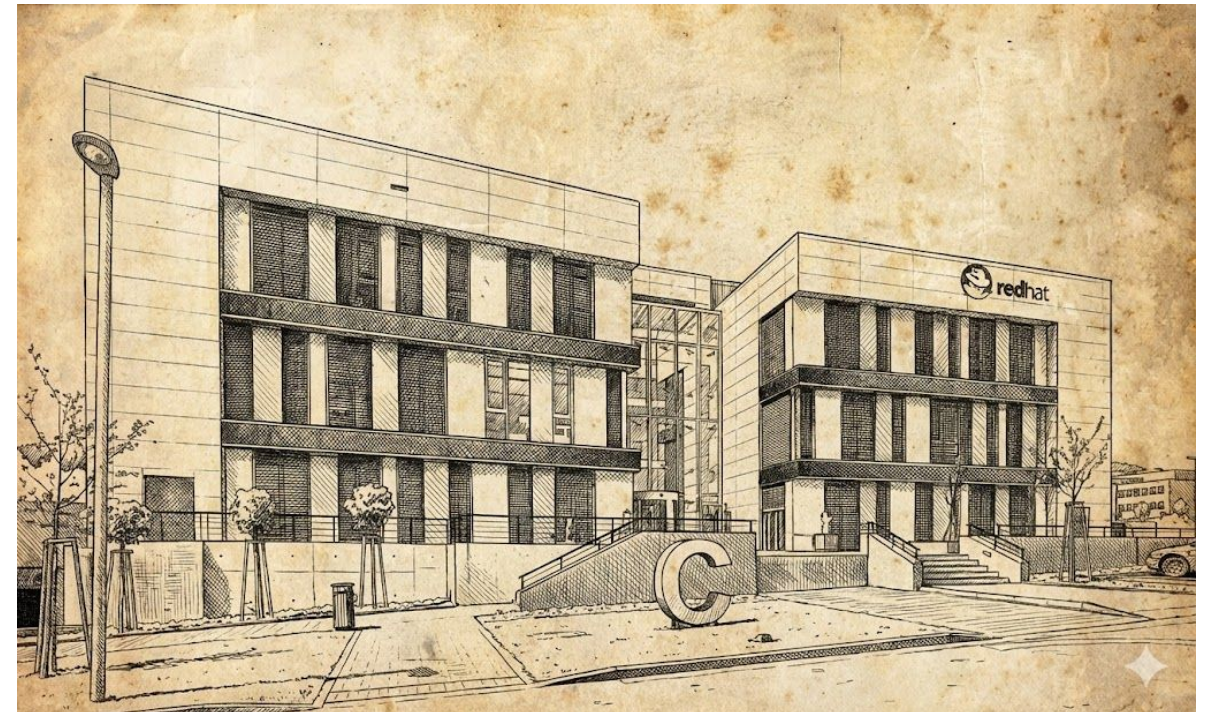
Milestone 2: 31.12.2030

- Next Steps:
 - Support cryptographic agility and a quantum-safe upgrade path.
 - Allocate resources for the transition.
 - Adapt certification schemes.
 - Evolve the rules.
 - Look for opportunities within the ecosystem.
 - Considering transversal activities throughout the creation and implementation of the roadmap.
 - Implement pilot use cases and contribute to testing centres.
- Main achievements:
 - The PQC transition for high-risk use cases has been completed.
 - PQC transition planning and pilots for medium-risk use cases has been completed.
 - Quantum-safe software and firmware upgrades are enabled by default.

Co se stane

Svět půjde kupředu

- ▶ Open-Source bude postupně umět PQC bez ohledu na ty, kterým je to jedno.
- ▶ Red Hat vede snahu o zavedení PQC i díky inženýrům z Brna
- ▶ PQC chcete mít zavedené co nejrychleji



Děkuji za pozornost



linkedin.com/company/red-hat



youtube.com/user/RedHatVideos

```
cloud@docke:~  
[matej@matej-mrazak ~]$ ssh second  
** WARNING: connection is not using a post-quantum key exchange algorithm.  
** This session may be vulnerable to "store now, decrypt later" attacks.  
** The server may need to be upgraded. See https://openssh.com/pq.html  
Activate the web console with: systemctl enable --now cockpit.socket  
  
Last failed login: Thu Nov 20 22:16:50 EST 2025 from 129.212.190.206 on ssh:nott  
y  
There were 2 failed login attempts since the last successful login
```