Raiffeisen Bank

# Kvantové počítače: Víc než jen kočka v krabici

Připravte se na svět, kde mohou kvantové počítače snadno prolomit dnešní šifry. Začneme **qubitem** – kvantovým bitem, který na rozdíl od Schrödingerovy kočky není jen paradoxem, ale dává kvantovým počítačům jejich exponenciální výpočetní sílu.

Probereme **Shorův algoritmus**, který mohou kvantové počítače využít k prolomení současných šifrovacích metod, a ukážeme si, jaký dopad to může mít na dnešní bezpečnost dat.

Objasníme důležitost **retroaktivní kryptoanalýzy** – co bylo jednou odesláno, už nelze vzít zpět.

Nakonec se podíváme na **postkvantové algoritmy**, které představují řešení odolné vůči kvantovým útokům. Tato změna bude mít zásadní dopad na budoucnost IT bezpečnosti a rozhodně to nebude jen běžný „update".

**TOMÁŠ ROSA**
vedoucí kryptologického kompetenčního centra RBI

**Kdy?**
15. 10. 2024 od 17:30

**Kde?**
Kavárna Šestnáctka

Budova City Tower
Hvězdova 1716/2b
Praha 4 – Pankrác

**V případě zájmu se registrujte** přes tento registrační formulář.

## Na co se můžete **těšit**?

**Na diskuzi s naším odborníkem Tomášem Rosou**, networking s lidmi z Raiffky a s dalšími studenty. A možná i na zásadní inspiraci pro svou kariéru.

**Na seznámení s Raiffkou zevnitř**, které se naskytne málokomu, návštěvu prostor v nejvyšší kancelářské budově Prahy a pohled na metropoli jako z letadla.