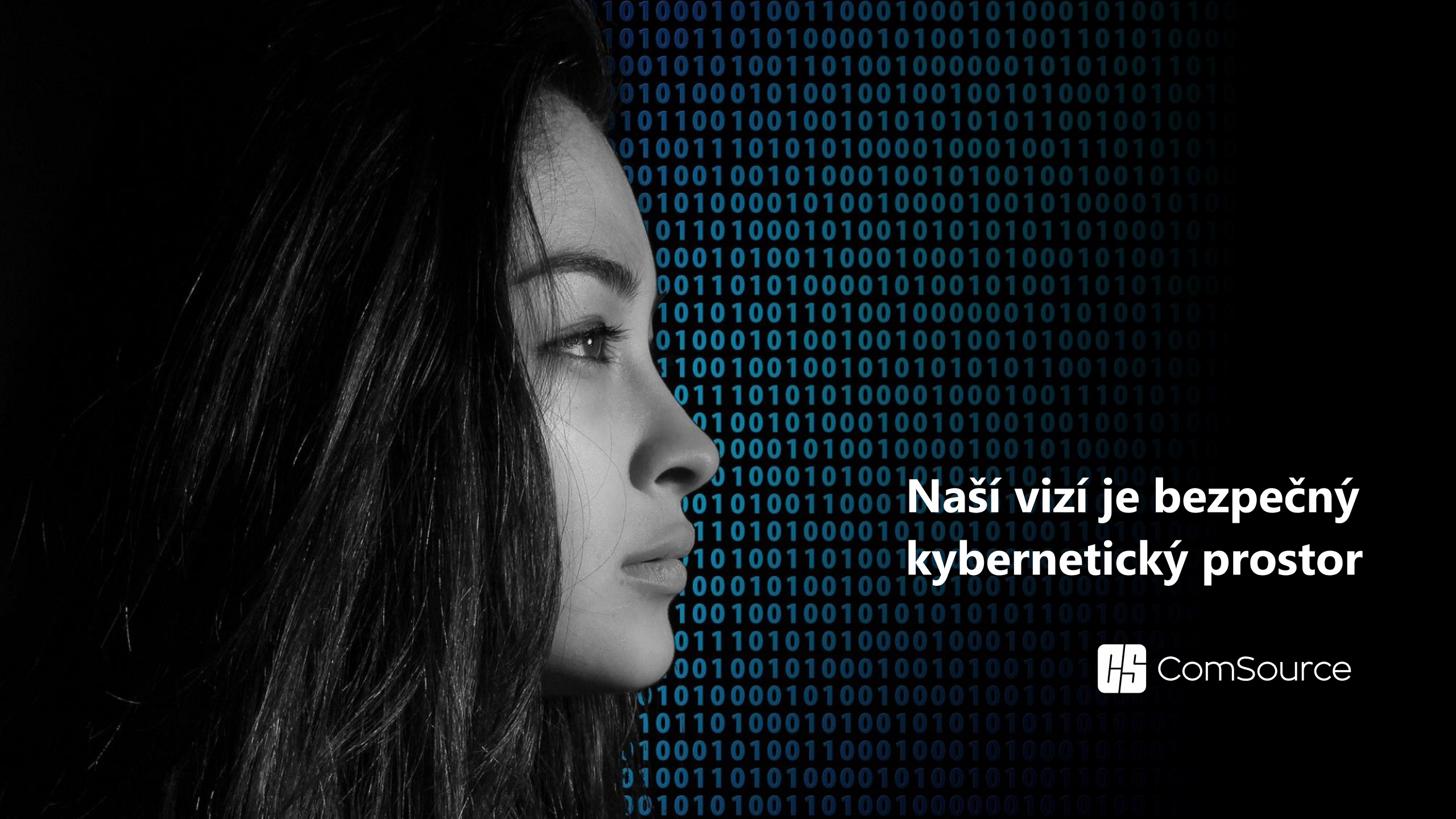
ComSource

Budoucnost v kybernetickém prostoru nevážně vážně

Prezentuje: Marek Kocan


Naší vizí je bezpečný
kybernetický prostor
ComSource

ComSource

- Specializace na několik pečlivě vybraných vendorů.

ComSource partnerství

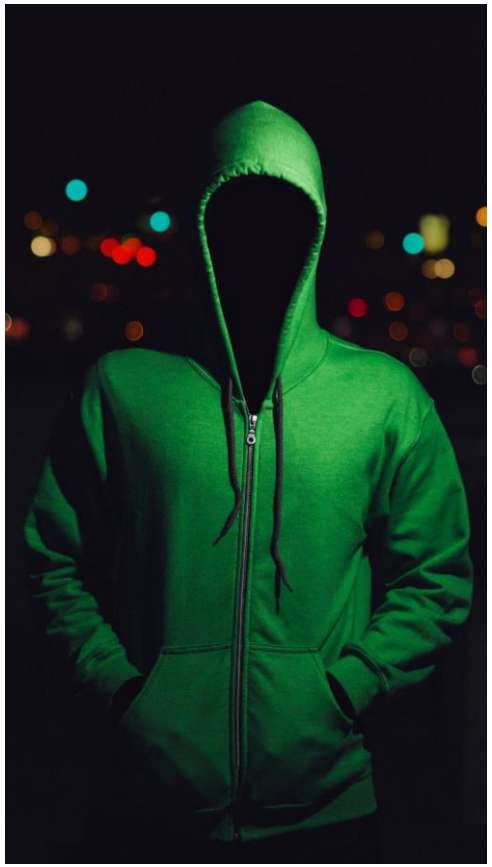
Jsme součástí týmu CSIRT (Computer Security Incident Response Team). Úkolem národního týmu CSIRT.CZ je ve spolupráci s Národním bezpečnostním úřadem reagovat, koordinovat a řešit bezpečnostní incidenty v oblasti bezpečnosti IT.

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.

Pocity přetížení / ohrožení v digitálním světě

Budoucnost



- Faktory nejistoty a rychlosti změn:
  - technologické zlomy (kvantové počítače, AI …)
  - geopolitické vlivy (války, boj o data …)
  - … ale také lidský faktor (adaptace na nové podmínky) …
- Od optimismu přes realismus až po pesimismus
- Máme šanci poznat bod zlomu nebo již nastal?
- Pohledy do nedávné minulosti:
  - internet – svoboda vs. dezinformace a kyber-podsvětí
  - chytré telefony – lepší komunikace vs. totální digitalizace, ztráta soukromí
  - cloudy – snadný přístup vs. vektory vedoucí k naprostému kolapsu
  - …
- Školství – samotné prostředí / formování budoucích „obětí“

Umělá inteligence ??????

- *Schopnost strojů napodobovat lidské schopnosti, jako je uvažování, učení se, plánování nebo kreativita*
- Dnes používaná umělá inteligence není "skutečná" umělá inteligence ve smyslu schopnosti myslet, chápat nebo jednat jako člověk:
  - Chybí obecná inteligence
  - Neexistence vědomí a pochopení
  - Závislost na datech a předem vytvořených modelech
  - Žádná kreativita v pravém slova smyslu
  - Neschopnost chápat morální a etické kontexty
- Dozvíme se vůbec, až bude AI skutečná I?

AI a ofenzíva

- Generování škodlivého kódu
- Personalizace škodlivého obsahu
- Příprava věrohodných phishingových kampaní
- Tvorba uvěřitelných deepfakes
- Šíření dezinformací a manipulace s veřejným míněním
- Odhalení zranitelností a pokročilá analýza chování
- Vyhledávání vhodných cílů pro útok
- Obcházení bezpečnostních mechanismů
- Optimalizace útoků
- Útoky na samotné UI (cílem je např. generování chybných informací, DDoS)
- Vyhodnocování efektivity

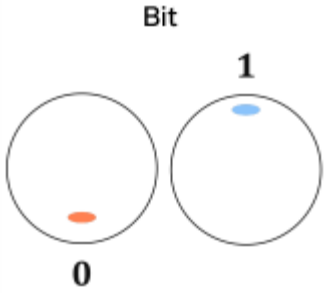
AI a defenzíva

- Pokročilá analýza stavů (například fragmenty malware, ne signatury!)
- Odhalení zranitelností a špatných konfigurací
- Analýza obsahu (například u phishingu, odhalení deepfakes)
- Pokročilá analýza chování (programů, uživatelů, komunikace)
- Obecné propojení zdánlivě nesouvisejících událostí a stavů
- Klasifikace citlivých dat
- Vyhodnocování logů a událostí (log management, SIEM …)
- Vyhodnocování informací z reputačních zdrojů
- Monitoring IoT
- Prediktivní analýza – pozor, asi se stane to a to…
- Podpora automatizace (reakce na události/incidenty/patchování)
- Vyhodnocování efektivity

Přišlo kvantum – a vše může být jinak!

Tradiční počítačový svět

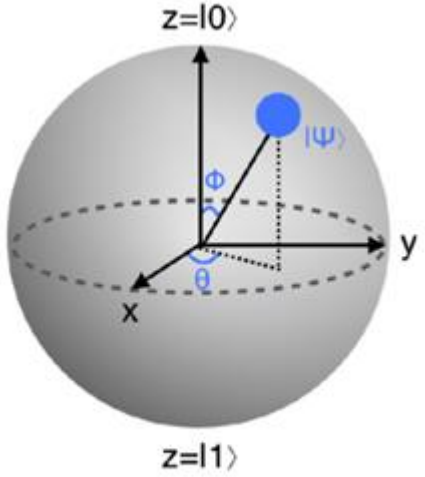
- Analogové technologie
- Digitální technologie
  - využití tranzistorů
  - bity - nuly a jedničky



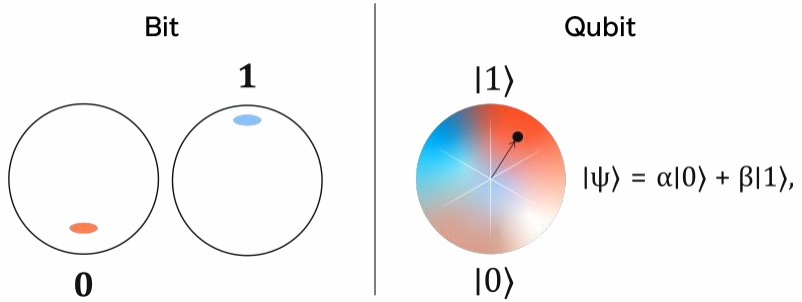
- Přesvědčení, že co nelze v rozumném čase a za rozumných nákladů vyřešit pomocí 0 a 1, nelze vyřešit vůbec

Kvantový svět

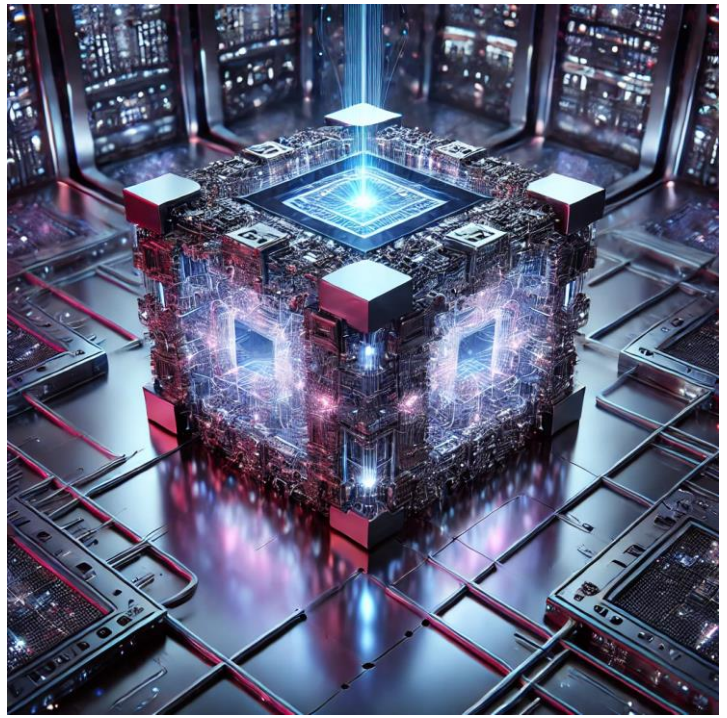
- Zcela nový přístup
- Bity „končí, přichází“ qubity
- Základem kvantových bitů jsou jevy kvantové fyziky
- Nejde jen o nuly a jedničky, ale o (kvantovou) superpozici těchto dvou stavů



qubit



Kvantový svět



- Neřešitelné pomocí nul a jedniček se stane řešitelným (v rozumném čase a za rozumných nákladů) aneb kvantová nadřazenost
- 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)
- Problémy stabilita, chyby, chlazení …
- Speciální algoritmy – Groverův (vyhledávání v nestrukturovaných datech), Shorův (faktorizace velkých čísel na prvočísla) …

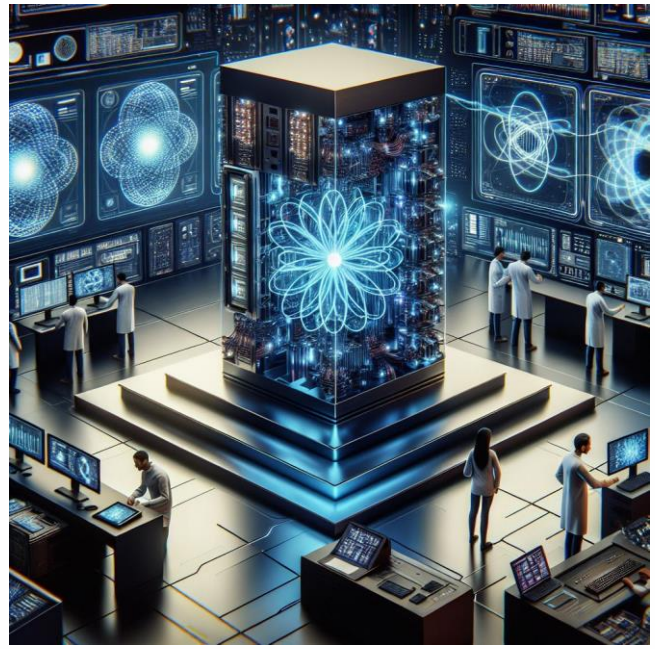
Kryptografie a kvantový svět

- Symetrické šifry – při dostatečné délce klíčů OK
  - AES-128, 192 nebo 256
- Asymetrické šifry – problém je paralelní výkon
  - RSA, ECC, DSA … nebudou bezpečné
- Uložená data -> relativně snadná opatření
- Přenášená data -> stávající algoritmy nebudou stačit
- Máme se bát?
  - RSA-2048, potřeba cca 4000 qubitů, IBM cca 10k qubitů do konce této dekády

Shorův algoritmus

- Peter Williston Shor 1994
- Jeden z neznámějších kvantových algoritmů
- Efektivní faktorizace velkých čísel aneb hledání součinu prvočísel
- 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

Postkvantová kryptografie

- Kryptografie odolná vůči útokům pomocí kvantových počítačů (pozor: Harvest now, decrypt later)
- Využití tradičních počítačů a lepších algoritmů
- Nejde tedy o kvantovou kryptografii (např. Quantum Key Distribution)
- 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
- EK: Doporučení pro koordinovanou implementaci přechodu na PQC (4/2024)
- NÚKIB: Kvantová hrozba a kvantově odolná kryptografie, příloha dokumentu *Minimální požadavky na kryptografické algoritmy* (2/2025)

My nevíme ...

Digitální stopa

- Pasivní digitální stopa
  - připojení k síti (pevný internet i WiFi)
  - informace o komunikaci v rámci internetu a dalších sítí
  - automatické sledování polohy
  - interakce na sociálních sítích (bez příspěvků!!)
  - sběr dat ze strany chytrých zařízení / IoT
- Pasivně/aktivní digitální stopa
  - elektronická pošta
  - souhlasy s analýzou dat na cloudových službách
  - metadata v souborech (např. ve fotkách)
  - přihlášení ke službě
  - informace z veřejně dostupných zdrojů (např. katastr)
- Aktivní digitální stopa
  - registrace a profily
  - příspěvky na sociálních sítích, nahrávání videí
  - komentáře u článků (pozor, stačí lajk)
  - historie vyhledávání
  - nákupy, hodnocení, recenze
  - účast v on-line hrách
  - přidávání informací o pracovních zkušenostech

Legislativní rámec aneb povinná stopa

- Sběr provozních a lokalizačních údajů (Data Retention)
- Směrnice Evropské unie 2006/24/EC
- Zákon o elektronických komunikacích
- Vyhláška o uchovávání, předávání a likvidaci provozních a lokalizačních údajů
- Letmý náhled pro službu přístupu k internetu z pevného připojení
  - *typ připojení*
  - *telefonní číslo nebo označení uživatele*
  - *identifikátor uživatelského účtu*
  - *adresa MAC zařízení uživatele služby*
  - *datum a čas zahájení a ukončení připojení k internetu*
  - *označení přístupového bodu u bezdrátového připojení k internetu*
  - *adresa IP a číslo portu, ze kterých bylo připojení uskutečněno*

Proč nás to trápí?

- Vliv na soukromí, a to i zpětně
- Izolace, diskriminace, stres, úzkost, kybernetická šikana -> sebevraždy
- Zneužití pro marketing i kybernetický zločin (vydírání …)
- Vytěžování informací ze sociálních grafů
- Krádež / falšování identity
- Ovlivnění digitální reputace
- Zneužívání mj. v právních sporech
- Ztráta anonymity
- Nemožnost úplného odstranění
- … ale také digitální vyhoření

- … a odhalení lží (mami, já fakt byl ve škole vs. fotka na instáči z kina)

Jak se nezbláznit?

- Dodržovat obecná pravidla pro pohyb v kybernetickém prostoru
- Vyváženost prevence a vzdělávání
- Vnímat pravidla a opatření jako pomoc, ne jako nepřátele
- Skutečně pochopit opravdový smysl jednotlivých opatření
- V nových technologiích hledat naději, ne hrůzu a obavy
- Důvěřovat, ale prověřovat
- Získat ponaučení z dosavadních událostí a incidentů
- Postupně se zdokonalovat, ne „odezdizmu“
- !!!ZDRAVÝ ROZUM a NEPROPADAT PANICE!!!
- A jít se projít ven a užívat normálního života

Otázky?

ComSource

Děkuji za pozornost

Email: marek.kocan@comsource.cz

Tel: 604 766 243