Základy analytického psaní v oblasti kyberbezpečnosti

Luboš Přikryl

Něco málo o mě

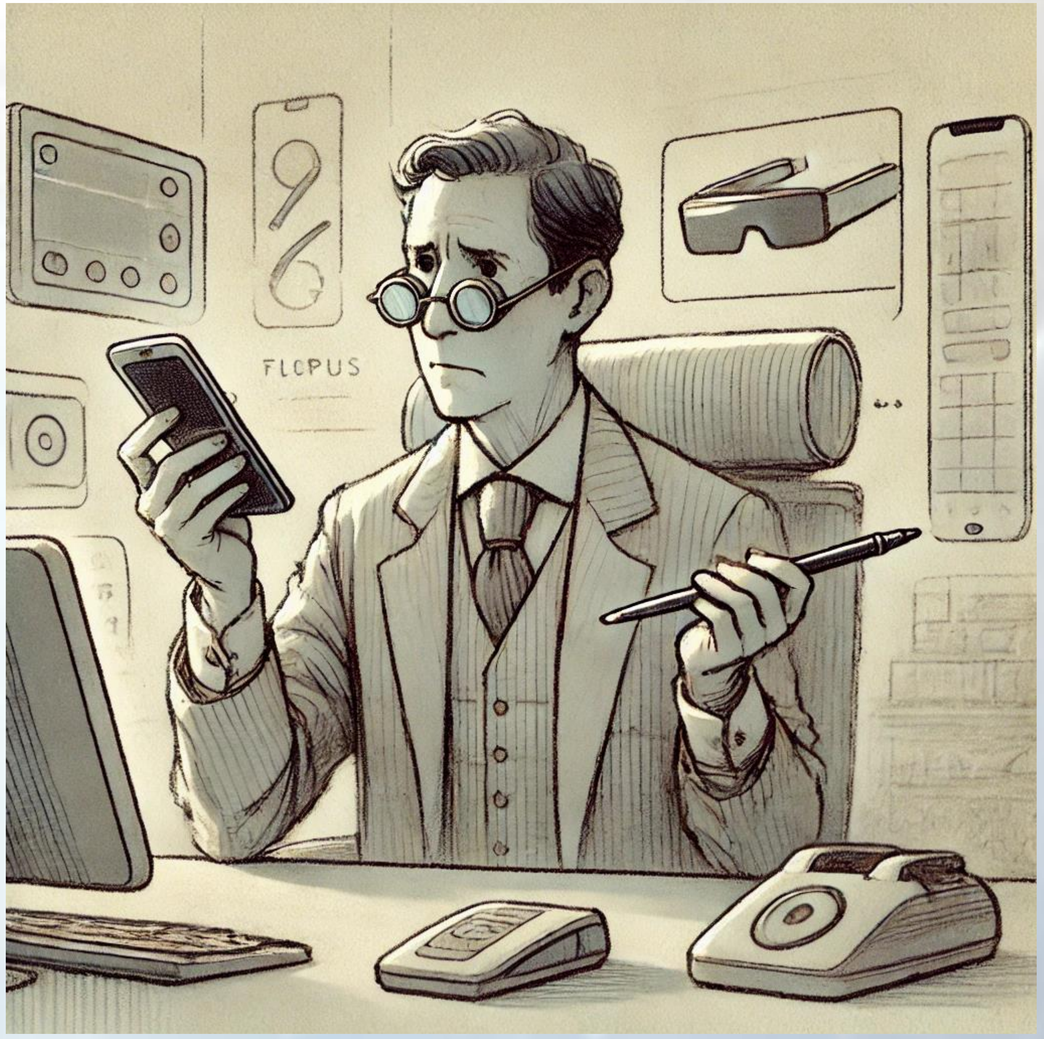
- Aktuálně doktorát na FSS
- Předtím BSS Bc. a Mgr.
- Pět let na NÚKIB
- Zaměření na EDTs
- Analytické výstupy
- OCA/OSA

Cena informace

- Cena jakou informace má je daná tím ke komu se dostane
- Najdete zranitelnost, incident, útok
- A co teď?
- Informace musí najít správné uši
- Různí lidé potřebují různé informace
- Musíte se rozhodnout co komu řeknete, jak, a v jakém kontextu
- Měsíce excelentní technické práce můžou přijít vniveč, když se nedostanou ke správnému adresátovi

Váš šéf nebude Ajťák

- I v případě že nebudete psát reporty navenek
- Jednoho dne velmi pravděpodobně narazíte na laika
- V soukromém i ve státním
- Dřív nebo později
- A i kdyby ne, vaši klienti nebudou
- Umět psát pro ne-IT lidí se bude hodit



Nikdo nechce číst vaše *píp*

“Nobody Wants to Read Your Sh*t”

Readers need to invest time and attention

Streamline your message, focus it and pair it down

Make it so **interesting**, that the reader would have to be crazy NOT to read it

Vaše publikum

- Vesměs se dá rozdělit do tří kategorií
  1) Lidi z branže
  2) Veřejnost
  3) Decisionmakeři

Kolegové z branže

- Organizace na vaší úrovni
- Co je zajímá?
- Technické informace
- Pravděpodobně mají plné pochopení kontextu
- Dají si čas na to přečíst velkou technickou analýzu
- Váš cíl: sdílet klíčové informace a know-how

Veřejnost

- Váš běžný člověk z ulice (eventuelně zákazník)
- Co ho zajímá?
- Laické termíny
- Má jen malé povědomí o kontextu
- Může si dát čas něco přečíst, ale musí ho to zaujmout
- Váš cíl: předat informace o tom co děláte (jak ve státním tak v soukromém)

Decisionmakeři

- Politici, vysocí funkcionáři, kravaťáci…a vaši nadřízení.
- Co je zajímá?
- Klíčový je kontext („Proč by mě to mělo zajímat?“)
- Chápe málo z kontextu
- A má plný itinerář jiných problémů
- Váš cíl: Dát mu podklady pro dobré informované rozhodnutí (a ospravedlnit svou existenci ☺)

Case study – Donald Trump

- ▪ Trump rád studuje vizuální pomůcky — mapy, grafy, obrázky a
- videa, stejně jako “killer graphics”, Mike Pompeo, bývalý ředitel CIA
- ▪ “Mám rád odrážky nebo maximální stručnost”
- ▪ “Nepotřebuji, vždyť víte, 200 stránkovou zprávu o něčem, co může být zvládnuto na jedné stránce”
- ▪ Zvyky realitního magnáta, který pracoval s plány budov a vizualizacemi toho, jak budou vypadat
- ▪ “pictures do say a thousand words”

Deset přikázání

- Bývalý vedoucí našeho analytického oddělení vytvořil 10 přikázání dobré analytické praxe.
- Sestaveno na základě knih bývalých pracovníků zpravodajských služeb z celého západního světa
- Nemusíte se jimi řídit, můžete si vytvořit vlastní, ale obecně dojdete ke stejným závěrům

Deset přikázání

- HLAVNÍ SDĚLENÍ

Zamyslete se nad tím, jaké je hlavní sdělení výstupu. Jakou hlavní message si má čtenář (resp. decision-maker) odnést. V textu jí zdůrazněte: v názvu výstupu, ve shrnutí, v rámci BLUF.

- BOTTOM LINE UP FRONT (BLUF)

Hlavní sdělení je vždy na začátku produktu, na začátku každé kapitoly i odstavce (BLUF). Až v další části rozvíjíte argumenty a dodáváte podpůrná tvrzení. Tj. opak toho, co nás učili na VŠ.

Deset přikázání

- VÝSTIŽNÉ SHRNUTÍ

Ve shrnutí je zachycena hlavní message výstupu a relevance pro ČR. Zamyslete se nad tím co je to nejdůležitější, co by si měl čtenář zapamatovat - **včetně vašeho odhadu dalšího vývoje.**

- ANALYTICKÝ NADPIS

Nadpisy nesmí být jen suchým popisem toho o čem výstup nebo kapitoly jsou, ale musí obsahovat i analytické sdělení.

Deset přikázání

- NÁZEV A SHRNUTÍ FUNGUJÍ I SAMOSTATNĚ

Název výstupu a nadpisy kapitol jsou pro toho, kdo má 5 vteřin (šéf šéfů). Proto i nadpisy musejí obsahovat analytické sdělení.

Shrnutí je pro toho kdo má 50 vteřin (náměstek). Hlavní text je pro toho, kdo má 5 minut a více (ředitel odboru). A přílohy pro toho, kdo má 15 minut a více (odborný pracovník).

- OBRÁZKY, MAPY, TABULKY, VIZUALIZACE

Hojně využívejte obrázky, fotografie, mapy, vizualizace dat a tabulky tak, abyste udělali váš výstup vizuálně přitažlivý. **Žádná stránka nesmí být jen jednolitý text**

Deset přikázání

- ANALYTICKÉ OTÁZKY – ZÁKLAD STRUKTURY VÝSTUPU

Identifikujte analytický problém. Téma by mělo být natolik specifické, aby obsahovalo nějakou změnu či pohyb.

Analytický problém rozložte na základní analytické otázky:

- Co se děje nového či odlišného?
- Proč se to děje?
- Co jsou cíle hlavního aktéra událostí?
- Jaké faktory ovlivňují, zda aktér uspěje nebo ne?
- Jaké jsou implikace pro ČR?
- Co se bude dít dále?

Deset přikázání

- IMPLIKACE, VÝHLED A DOPORUČENÍ

Neprezentujete informace, ale jejich interpretaci. Nepřemýšlejte nad tím jak popsat co se stalo, ale jak vysvětlit **co dané události znamenají pro zákazníka** a jaký bude podle vašeho odhadu další vývoj. Podáte **vysvětlení hlavních sil**, které událost řídí a faktorů, na nichž tyto síly závisí.

Postupně tak čtenáři v samostatných kapitolách vysvětlíte co se děje, co se bude dít dále, co to pro něj znamená, a doporučíte mu vhodná opatření (technická i policy) navazující na analytická zjištění.

Ve zkratce: Jak řešit problém se kterým analýza přišla

Deset přikázání

PEER REVIEW

Výstupy vždy konzultujte s kolegy z dalších částí úřadu. Vyhledáváme připomínky a oponenturu.

VYUŽÍVEJTE PŘÍLOHY

Pro informačně přínosné, ale v zásadě deskriptivní části využívejte přílohy – např. pro popisy jednotek či organizační struktury nějakého aktéra. Pokud je popis stručný a důležitý, můžete jej nechat v rámečku v hlavním textu.

Pro každý výstup si definujte jedno nebo dvě **hlavní sdělení**

Definujte si, **co** vaší analýzou **chcete** zákazníkovi **říct**

Co by si měl zapamatovat, aby mohl udělat **informované rozhodnutí**

Pravděpodobnost

PRAVDĚPODOBNOSTNÍ VÝRAZY NÚKIB

Výraz	Pravděpodobnost
Téměř jistě	*90–100 %*
Velmi pravděpodobně	*75–85 %*
Pravděpodobně	*55–70 %*
Nelze vyloučit/Reálná možnost	*40–50 %*
Nepravděpodobně	*20–35 %*
Velmi nepravděpodobně	*0–15 %*

- Existuje mnoho různých frameworků
- Co důvěra?
- Moc „střední cesty“?

Utajení

- Pokud budete ve státním, částečně to kryje zákon
- Ale i zákonem neregulované dokumenty (státní i korporátní) by měly mít nějaká pravidla
- TLP protocol

Měsíční přehled incidentů

TPL:WHITE

Měsíční přehled incidentů

- Každý měsíc
- Jak česká tak anglická verze
- Základní přehled incidentů za měsíc
- Trendy a infografiky
- Krátká analýza nějakou současného trendu
- Může souviset s konkrétním incidentem, ale nemusí (edukativní rozměr)

Měsíční přehled incidentů

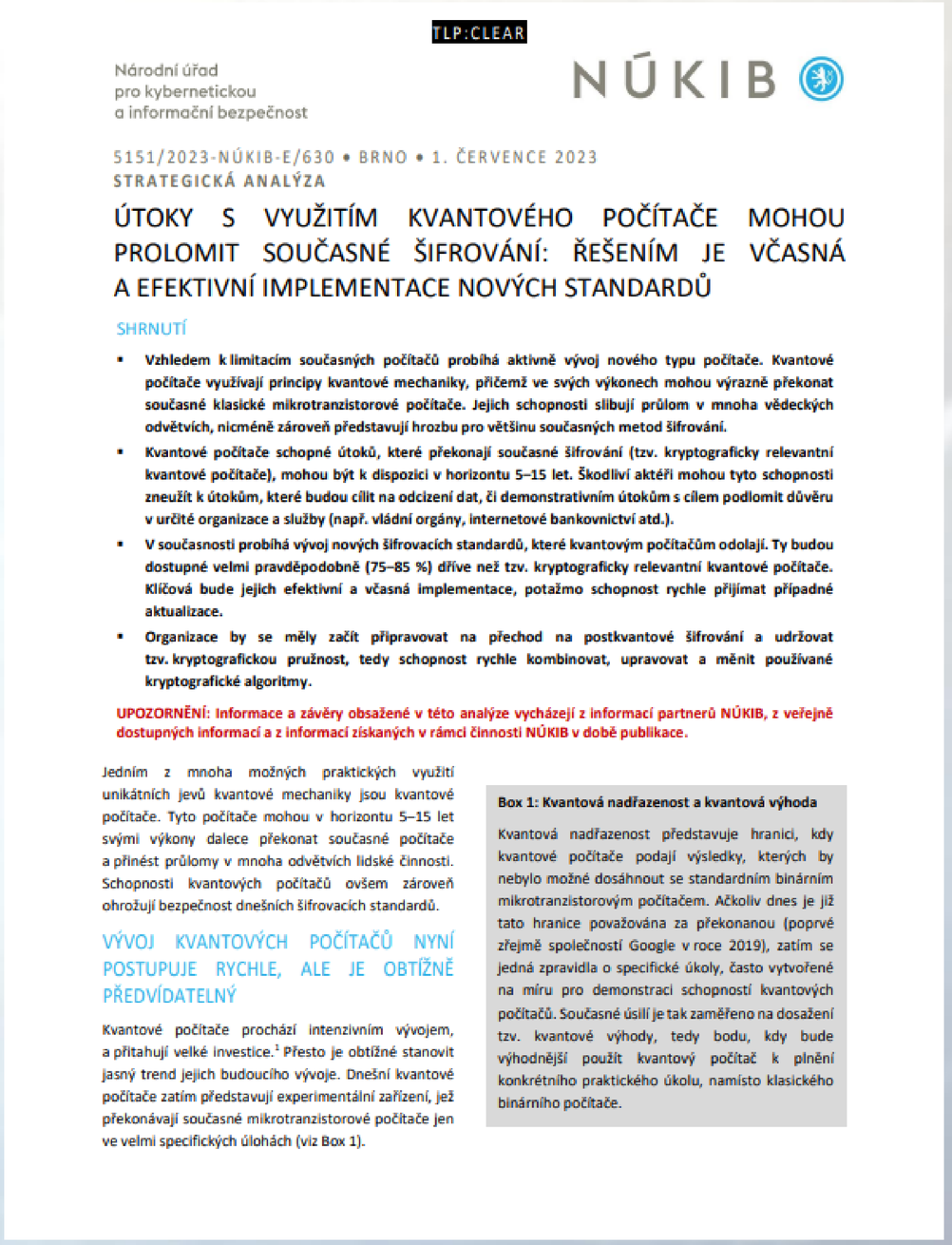
- Jaké incidenty reportujeme?
- Nejmenujeme oběti (ani když je to známý případ)
- Nereportujeme „živé případy“
- Neatribuujeme útočníky
- …většinou

Strategická analýza

Utoky s vyuzitim kvantoveho pocitace mohou prolomit sousasne sifrovani resenim je vcasna a efektivni implementace novych standardu.pdf

Strategická analýza

- Středně velký produkt
- Neperiodický
- Zaměřený na nějaké téma
- Publikum se může lišit
- Různé stupně důvěrnosti



TLP:CLEAR

Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

5151/2023-NÚKIB-E/630 • BRNO • 1. ČERVENCE 2023

STRATEGICKÁ ANALÝZA

ÚTOKY S VYUŽITÍM KVANTOVÉHO POČÍTAČE MOHOU PROLOMIT SOUČASNÉ ŠIFROVÁNÍ: ŘEŠENÍM JE VČASNÁ A EFEKTIVNÍ IMPLEMENTACE NOVÝCH STANDARDŮ

SHRNUTÍ

- **Vzhledem k limitacím současných počítačů probíhá aktivně vývoj nového typu počítače. Kvantové počítače využívají principy kvantové mechaniky, přičemž ve svých výkonech mohou výrazně překonat současné klasické mikrotranzistorové počítače. Jejich schopnosti slibují průlom v mnoha vědeckých odvětvích, nicméně zároveň představují hrozbu pro většinu současných metod šifrování.**
- **Kvantové počítače schopné útoků, které překonají současné šifrování (tzv. kryptograficky relevantní kvantové počítače), mohou být k dispozici v horizontu 5–15 let. Škodliví aktéři mohou tyto schopnosti zneužít k útokům, které budou cílit na odcizení dat, či demonstrativním útokům s cílem podlomit důvěru v určité organizace a služby (např. vládní orgány, internetové bankovnictví atd.).**
- **V současnosti probíhá vývoj nových šifrovacích standardů, které kvantovým počítačům odolají. Ty budou dostupné velmi pravděpodobně (75–85 %) dříve než tzv. kryptograficky relevantní kvantové počítače. Klíčová bude jejich efektivní a včasná implementace, potažmo schopnost rychle přijímat případné aktualizace.**
- **Organizace by se měly začít připravovat na přechod na postkvantové šifrování a udržovat tzv. kryptografickou pružnost, tedy schopnost rychle kombinovat, upravovat a měnit používané kryptografické algoritmy.**

UPOZORNĚNÍ: Informace a závěry obsažené v této analýze vycházejí z informací partnerů NÚKIB, z veřejně dostupných informací a z informací získaných v rámci činnosti NÚKIB v době publikace.

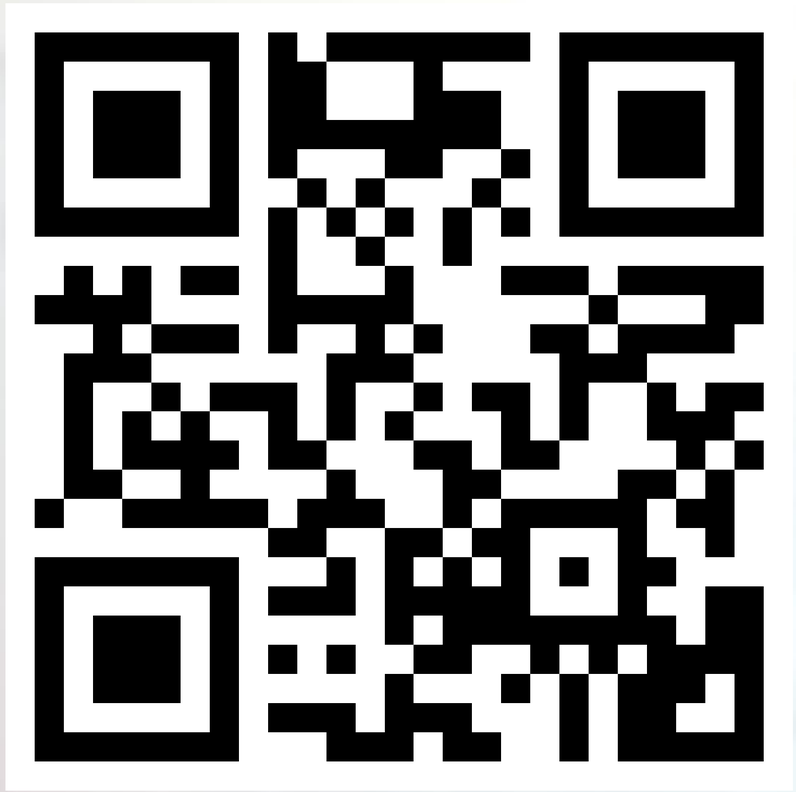
Jedním z mnoha možných praktických využití unikátních jevů kvantové mechaniky jsou kvantové počítače. Tyto počítače mohou v horizontu 5–15 let svými výkony dalece překonat současné počítače a přinést průlomy v mnoha odvětvích lidské činnosti. Schopnosti kvantových počítačů ovšem zároveň ohrožují bezpečnost dnešních šifrovacích standardů.

VÝVOJ KVANTOVÝCH POČÍTAČŮ NYNÍ POSTUPUJE RYCHLE, ALE JE OBTÍŽNĚ PŘEDVÍDATELNÝ

Kvantové počítače prochází intenzivním vývojem, a přitahují velké investice.[1] Přesto je obtížné stanovit jasný trend jejich budoucího vývoje. Dnešní kvantové počítače zatím představují experimentální zařízení, jež překonávají současné mikrotranzistorové počítače jen ve velmi specifických úlohách (viz Box 1).

Box 1: Kvantová nadřazenost a kvantová výhoda

Kvantová nadřazenost představuje hranici, kdy kvantové počítače podají výsledky, kterých by nebylo možné dosáhnout se standardním binárním mikrotranzistorovým počítačem. Ačkoliv dnes je již tato hranice považována za překonanou (poprvé zřejmě společností Google v roce 2019), zatím se jedná zpravidla o specifické úkoly, často vytvořené na míru pro demonstraci schopností kvantových počítačů. Současné úsilí je tak zaměřeno na dosažení tzv. kvantové výhody, tedy bodu, kdy bude výhodnější použít kvantový počítač k plnění konkrétního praktického úkolu, namísto klasického binárního počítače.



ZSKB

ZSKB

- Píše OSA
- S přispěním všech pracovníků agentury
- Hlavní publikace našich aktivit
- Pověření vládou a zákonem
- Musí být schválena vládou
- Veřejná
- CZE i ENG

The big dilema of translation

- Umíte psát anglicky?
- Bude vám to dovoleno?
- Nejlepší řešení je snadné na papíře...ale je těžké ho získat
- Outsourcing?
- Lidem nebo umělé inteligenci?
- Je to bezpečné (a legální)?

Používat AI?

- Vypomáhat si AI je v pohodě
- Ale…ale
- Vaše výstupy budou kombinací textu, obrázků, stylisticky atd…
- AI vám pomůže s dílčími úkoly
- Hlavní problém je ale citlivost dat

Prostor pro dotazy