# Potřeba průkazné informatiky

**Radek Beneš**
**Znalec informačních technologií**
**Konference itSMF, ČSSI, leden 2015**

# proč tato přednáška

Bezpečnostní incident často končí vlastním, či externím vyšetřováním, a to s potřebou průkazného (objektivního) dokazování u orgánů činných v trestním řízení, či orgánů soudních.

Většina společností, stejně jako různé metodologie řízení IT (bezpečnost, rizika) ale podceňují tvorbu a uchovávání digitálních stop.

Jak jste připraveni na vyšetřování Vy?

# některé statistiky

- „Počítačová kriminalita rok od roku roste. Veřejnost nejvíce ohrožují internetové podvody. Za poslední měsíce jich přibyly stovky! Ještě v roce 2011 jsme v České republice evidovali bezmála 880 trestných činů podvod, které se uskutečnily v rámci internetu. O dva roky později jich už byl více než dvojnásobek!“, uvedla 30. ledna 2014, mjr. Ing. Jana Macalíková, tisková mluvčí Policejního prezidia ČR.
- Společnost PwC provedla celosvětový průzkum hospodářské kriminality 2014. Výsledky této studie potvrzují, že hospodářská kriminalita v České republice se stává čím dál běžnějším jevem a bere na sebe rozmanitější podoby. Podvody v nákupním procesu či počítačová kriminalita se postupně staly samostatnými hlavními kategoriemi podvodu, kdy každá druhá firma v Česku se stala obětí hospodářské kriminality (každá 4 obětí zaměstnanců).

# některé definice

- **Počítačová kriminalita (cyber-crime)** je trestná činnost, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení (včetně dat), nebo pouze některá z jeho komponent, nebo počítačové sítě, a to jako předmět zájmu trestné činnosti, jako prostředí (objekt), nebo jako nástroj trestné činnosti.

  Pojem počítačová kriminalita se používá i pro tradiční formy kriminality, u níž byly počítače nebo počítačové sítě použity pro usnadnění (umožnění). Určujícím operacionálním elementem je přitom způsob zneužití výpočetní techniky, vzhledem k jejím specifickým vlastnostem a dominantnímu postavení mezi věcnými komponentami způsobu páchání konkrétního trestného činu.
- **Informační kriminalita (info-crime)** je taková trestná činnost, pro kterou je určující vztah k software, k datům, (uloženým informacím) respektive veškeré aktivity které vedou k neautorizovanému čtení, nakládání, vymazání, zneužití, změně nebo jiné interpretaci dat.
- **Kriminalita, související s pokročilými technologiemi (high-tech crime)** je taková trestná činnost, zaměřená na vyspělou techniku jako cíl, prostředí nebo nástroj pachatele trestného činu (zpravidla se jedná zároveň o aktivitu označitelnou za „počítačovou“ či „informační“ kriminalitu).

Obecně:

trestné činy zaměřené proti počítačům (ICT) nebo trestné činy páchané pomocí počítače (ICT)

„Nejde" o nový typ trestné činnosti, jen nové technologie a nové způsoby pro páchání už známých trestných činů

# znalec

„…v souladu

s koncepcí rovnosti zbraní musí být znalecký posudek hodnotitelný a kritizovatelný ze strany všech subjektů, které se podílejí na trestním procesu . . .“

# znalec

Znalecké zkoumání v procesu objasňování kriminalisticky relevantní události je samostatnou a specifickou metodou kriminalistické činnosti, spočívající v souhrnu úkonů, jejichž cílem je objasnění kriminalisticky relevantní skutečnosti ve formě znaleckého posudku nebo odborného vyjádření. Nezahrnuje pouze samotné znalecké zkoumání ani pouze znalecký posudek, ale je to proces utváření znaleckého důkazu, probíhající ve třech etapách:

# znalec

1. **Příprava a nařízení (objednávka) znaleckého zkoumání**

   Směřující k vytvoření předpokladu pro objektivní a úplné znalecké zkoumání. Zahrnuje činnosti:

- zajištění, shromáždění a dokumentace materiálu
- vymezení předmětu znaleckého zkoumání a výběr znalce
- sestavení a formulace úkolu (otázek) pro znalce
- nařízení (dožádání, ustanovení, objednávka) znaleckého zkoumání
- další spolupráce se znalcem

# znalec

**2. Vlastní znalecké zkoumání**

cílevědomé a systematické studium konkrétních objektů za použití odborných znalostí a odborných metod poznání, při kterém dochází k vydělování informací obsažených v kriminalistických stopách a jiných kriminalisticky relevantních objektech, za využití odborných znalostí z oblasti vědy, techniky, atp.

a) **Přípravné stadium** – znalec se seznamuje s předloženými materiály, ujasňuje si otázky, které bude řešit, určuje metody, prostředky, …

b) **Analyticko-syntetické stadium** – znalec podrobuje detailnímu zkoumání jednotlivé objekty, jejich vlastnosti a znaky, atp.

c) **Stadium vyvozování závěrů** – představuje závěrečné (vrcholné) stadium znaleckého zkoumání.

# znalec

**3. Hodnocení a využití výsledku ZP**

Výsledky znaleckého zkoumání mohou být použity jen na základě jejich objektivity, přesnosti a konkrétnosti, vylučující jakékoliv pochybnosti o způsobu jakým byly získány, o správnosti postupu znalce v průběhu zkoumání a o jím použitých metodách a prostředcích.

Proto ještě před vlastním využitím výsledku znaleckého zkoumání v procesu dokazování je orgán (např. činný v trestním řízení) povinen hodnotit jak vlastní závěry znalce, tak i jeho postup, jímž k závěrům dospěl.

# znalec

**Obecné hodnocení odborné správnosti ZP:**

- Hodnocení teor. východisek
- Hodnocení empirického základu posudku, tj. kvality a množství zjištěných znaků
- Hodn. použitých odborných metod a postupů
- Hodnocení, zda subsumpce konkrétního empirického základu pod obecný teoretický základ je správná

# znalec

V ČR není kompetentní orgán, nebo instituce, která by se forenzními vědami systematicky zabývala, a tudíž ani elementární problémy nemá kdo řešit.

# *Kyberkriminalita*

**Krádež identity (Identity Theft)**

Krádeží identity rozumíme krádeží osobních nebo finančních dat (např. čísla účtů) za účelem odcizení finančních prostředků nebo spáchání jakékoliv jiné trestné činnosti, vedoucí zpravidla k nejrůznějším podvodům.

**Sociální inženýrství (Social Engineering)**

Systematicky používá znalosti lidského chování, umění přesvědčování, aby uživatel udělal to, co by za normálních okolností, při dodržování všech bezpečnostních pravidel, nikdy neudělal. Tím je umožněn kybernetický útok.

# *Kyberkriminalita*

**Spyware**

Jde o nežádoucí SW - software (programové vybavení), který může poškozovat systémy, software, data, monitorovat chování uživatele a tyto informace předávat útočníkovi bez vědomí poškozeného.

**Cílené hrozby (Targeted Threats)**

Jedná se o kybernetické útoky s finanční motivací, jež jsou vedeny proti jedné instituci (firmě) nebo celému oboru (průmyslu). Nejsou zpravidla poškozenou společností (jednotlivcem, skupinou) publikovány.

# *Kyberkriminalita*

**Viry (Viruses)**

Škodlivé programy se zabudovaným mechanismem jejich šíření. Jakmile je jednou virový program spuštěn uživatelem, vykonává určitou z bezpečnostního pohledu negativní činnost a může se následně dále skrývat.

**DoS útoky (Denial of Service Attacks)**

Cílem těchto útoků je poškodit nebo vyřadit určité služby napadeného, například zahlcením velkým množstvím příchozích požadavků na zpracování dat, apod. DoS útoky mohou rovněž využít slabin systémů.

# Kyberkriminalita

**DNS útoky (DNS Attacks)**

Domain Name System ("směrování" v internetu) může být porušen nebo přesměrován na škodlivé web stránky. V poslední době jsou zaznamenávány útoky na lokální DNS služby, tzv. „pharming“.

**Hybridní červi (Hybrid Worms)**

Jsou to komplexní programy způsobující škody v informačním a komunikačním prostředí, využívající technologie běžných virů. Na rozdíl od virů jsou ale „samospustitelné“ a analyzují slabá místa SW nebo technologií.

# *Kyberkriminalita*

**„P2P“ útoky (Peer to peer Attacks)**

Peer to peer (P2P) prostředí umožňuje přenos virů a červů a znamená potenciální riziko jako jiná nechráněná síť. Mezi uživateli oblíbené komunikační prostředky patří například instanční messaging (IM) apod.

**Phishing, Rhybaření**

Využívá slabin samotného uživatele. Na něm jsou podvodným způsobem na základě věrohodného, ale falešného emailu či webového odkazu (spoofing) apod. vylákány citlivé osobní údaje, která jsou zneužita.

# *Kyberkriminalita*

**Nevyžádaná pošta (Spam)**

Nevyžádaná elektronická pošta poškozující uživatele nebo instituci. Nevyžádaný obsah může být mimo jiné vkládán i do internetových diskusních fór, rozesílány formou SMS, nebo MMS na mobilní zařízení, apod.

**Útoky na webové aplikace (Web Application Attacks)**

Zahrnuje soubor různých útoků na webové aplikace, jako například různé techniky skenování a zneužití slabých míst webového prostředí, ukládání do databáze, změny webových stránek (webfacing apod.).

# *Kyberkriminalita*

**Útoky na webové aplikace (Web Application Attacks)**

Zahrnuje soubor různých útoků na webové aplikace, jako například různé techniky skenování a zneužití slabých míst webového prostředí, ukládání do databáze, změny webových stránek (webfacing apod.).

**Útoky na aplikační úrovni (Application Level Attacks)**

Pod těmito hrozbami rozumíme aplikace vyvinuté a provozované v podniku (instituci) lokálně, nebo komerčně dodané, ale bez webového rozhraní. Aplikace webového charakteru jsou vedeny samostatně.

# *Kyberkriminalita*

**Botnety (Botnets)**

Botnety jsou množiny softwarových robotů (tzv. bots), které pracují v autonomním režimu mimo IT kontrolu napadeného prostředí. Případně propojené počítače, pod kontrolou útočníka, které využívá pro své cíle.

**Databázoví červi  (Database Worms)**

Sami se šíří, jsou cíleni na systém řízení relační databáze. Jsou schopni vyhledávat databáze, pokoušt se o přístup do ni a po přihlášení například zničit obrovský objem dat ve velice krátkém časovém období.

# *Kyberkriminalita*

**Finanční trojští koně (Financial Trojans Backdoor)**

Jedná se o škodlivý software typu trojského koně instalovaného do PC a speciálně určeného pro finanční podvody. Dochází k vkládání podvodných transakcí během komerčních transakcí s autentizací uživatele.

**Útoky na bezdrátové sítě (WLAN Attacks)**

K průniku do organizace může dojít pomocí nechráněné bezdrátové komunikace, která je obvykle připojena na vnitřní infrastrukturu. Může dojít k úniku velkého množství citlivých dat a to jak uložených, tak z komunikace samotné.

# *Kyberkriminalita*

**Reverzní inženýrství firemníchzdroj kódů (Ent. Code Rev. Eng.)**

Předmětem je reverzní analýza zdrojových kódů podnikových aplikací za účelem detekce zranitelnosti, technologického, procesního a algoritmického know-how, a nebo následného odcizení duševního vlastnictví.

**Hrozby webu 2. generace (Mashup Threats)**

Koncept Webu 2. generace umožňuje směšování obsahů různých zdrojů (web stránek) pomocí skriptování na straně browseru. Jde o zranitelnost skriptovaným útokům z různých zdrojů (web stránek).

# *Kyberkriminalita*

**Rootkity (Rootkits)**

Rootkit je modifikovaný systémový soubor, jež používají útočníci k záměně za původní, originální systémové soubory. Získávají kontrolu nad desktopem či serverem a není možné na úrovní admin. systému (root) detekovat průnik.

**Virtualizační hrozby (Virtualization Threats)**

Tyto hrozby jsou spojeny se zranitelností operačních systémů, využívajících virtualizační technologie, virtuální manažery, apod. Virtualizace je v IT budoucností, postupuje a nabývá na kvantitě i kvalitě.

# *Kyberkriminalita*

**Útoky na mobilní a bezdrátová zařízení (Mob. and W. Device Att.)**

Například i viry jsou rozšiřitelné na mobilní zařízení, např. telefony a jiné bezdrátová zařízení. Dále v případě krádeže těchto zařízení může dojít ke ztrátě citlivých dat nebo duševního vlastnictví.

**Generátory zákeřných kódů (Malicious Code Variants)**

Jedná se o generátory škodlivých kódů (virů, malware, spyware apod.). Rychle se generující velké množství kódů v rozličných variantách, jsou schopny dále prolomit některé antivirové a softwarové ochrany.

# *Kyberkriminalita*

**Zneužití malých kancel. nebo domácích aplikací (SOHO Vulnerabilities)**

Počet jejich instalací v praxi neustále roste, ale zároveň nejsou malé kancelářské nebo domácí aplikace dostatečně profesionálně podporovány, řízeny a zejména zabezpečeny. To vede k jejich velké zranitelnosti.

**… A DALŠÍ a další …**

# tvrzení

Při své profesní zkušenosti již nedělím společnosti (provozovatele ICT) na ty, které mají zkušenost s počítačovou kriminalitou a které nikoli, ale pouze již na ty, které problematiku řeší, nebo o ní nevědí (nepřipouštějí si ji).

# tvrzení

Při aktuálním nárůstu počítačové kriminality, resp. využití výpočetní techniky při trestné činnosti, se velmi pravděpodobně může stát, že se právě Vy, nebo Vaše společnost, bude potýkat s potřebou průkazného, objektivního a hodnověrného doložení např.: kdo s IT technikou manipuloval v čase, kdo pořídil (uložil, modifikoval, přenesl) určitá data, jak některý konkrétní software pracoval v dané době, kdo byl připojen ke konkrétnímu zařízení, síti, datům, jaké datové úložiště jsou užívána společností a která lze tedy identifikovat jako ne/autorizovaná, zda bylo s některými logy systémů manipulováno, atd. …

# digitální stopy

- Každé ICT zařízení, které vytváří, zpracovává, uchovává, nebo předává data, zanechává při své činnosti určité záznamy. Tyto záznamy lze z kriminalistického hlediska nazvat stopami, resp. digitálními stopami (dříve počítačovými stopami). V zahraniční literatuře lze narazit v tomto smyslu spíše na pojem „digital evidence“. Tento výraz v angličtině ale primárně spíše odpovídá významu „důkaz“ a zde přímo pramení i spojitá problematika, kdy důkaz je soudem akceptovaná, řekněme kvalitní, stopa. Má tedy určité atributy, kterým se budeme věnovat dále.

# digitální stopy

- Digitální stopy můžeme rozdělit alespoň do třech základních kategorií, a to z hlediska jejich využitelnosti a potřebné kvality:
- **Kriminalistické stopy** si lze představit ve vztahu k vyšetřování trestných činů a přestupků. U těchto stop vyžadujeme co nejvyšší míru kvality a objektivity. Kriminalistické stopy chápeme také jako podmnožinu tzv. forenzních stop.
- **Forenzní stopy** jsou takové, které jsou využitelné pro dané vyšetřování (jak kriminalistické, civilní i komerční sféře, včetně forenzních auditů), kdy je kladen důraz na to, aby výsledek vyšetřování, resp. interpretace, obstál i před soudními orgány (viz forenzní vědy a forenzní vyšetřování). U těchto druhů stop se vyskytují i stopy s nižší mírou objektivity (vlastní logy systémů, atp.).

# digitální stopy

V praxi dochází u těchto stop také k největší míře nenávratných škod v průběhu vlastních vyšetřování a auditů. Je potřeba si uvědomit, že zajištění originálů některých digitálních stop je neopakovatelným procesem a není možné, po některých zásazích, zajistit znovu forenzní stopy v dostatečné kvalitě, aby byly dále pro některé druhy řízení dostatečně průkazné a akceptovatelné.

- Poslední kategorií můžeme nazvat **jinak využitelnými stopami**. Sem řadíme již ostatní digitální stopy, které nemají logickou návaznost na forenzní stopy a nepodléhají výše uvedené kategorizaci. Jejich vznik je obvykle způsoben např. vnitřní kontrolou systémů a zařízení, atp., kdy obvykle tyto stopy nenesou významné atributy hodnověrnosti a nemohou být objektivně důkazně akceptována. Mohou poskytnout ale vodítka a další podklady pro směr dalšího zkoumání.

# digitální stopy

- Informace (digitální stopa) jako taková je nehmotná, pak v okamžiku jejího uložení se technologicky zhmotňuje na některou z forem paměťových médií, resp. datových úložišť, které má určité technologické provedení, jako např. formát, datovou strukturu, konektivitu, spolehlivost, automatickou a neovlivnitelnou tvorbu dalších informací, ne/přepisovatelnost, životnost, apod. Nad digitální stopou tedy prakticky vždy uvažujeme jako o stopě materiálního a hmotného charakteru, která vznikla biologickým, chemickým, fyzikálním působením, či kombinací uvedených.
- Dále je potřeba si uvědomit, že až na některé výjimky jsou digitální stopy tzv. mikrostopou, kdy nejsme schopni je svými smysly vnímat a potřebujeme určité interprety, software a technologické zařízení, abychom s nimi byli schopni pracovat.

# digitální stopy

- Vysoká obsažnost (lze získat data s velmi vysokou informační hodnotou. Uživatel obvykle využívá velkou šíři software a vybavení, které uchovává informace o tom co pořizoval, zpracovával, předával, uchovával, atp.
- Ne/heterogennost a ne/komplexnost prostředí (kdy v běžné praxi je běžné, že je provozováno paralelně několik prostředí, software, virtualizace, vzdálené úložiště, různé operační systémy, servery, zařízení, atp.).
- Časový údaj (kdy jednou ze základních charakteristik digitálních stop je obsah časového údaje s vysokou přesností, otázkou je z jakého zdroje a jak může být tento údaj ovlivněn).

# digitální stopy

- Geografický rozsah (kdy je v dnešní době běžné využití internetových služeb, on-line systémů, propojených počítačových sítí, kloudových úložišť, atd. Stopy se tak nemusí nacházet v lokálním prostředí, atp.)
- Ochrana (kdy v některých případech při vysokém stupni ochrany, někdy i necentralizovaně vložené do rukou samotných uživatelů, jsou data, resp. digitální stopy nečitelné, nepoužitelné, atp. i pro jejich majitele)
- Možnosti zahlazení (kdy systémy umožňují určitým uživatelům, při určitých technikách a právech zpětně modifikovat, mazat a vytvářet určité informace)

# digitální stopy

- Subjektivní faktory (vlivem použitých technologií, konfigurací, předpisy, právním rámcem, zálohováním, archivací, uživatelskými právy, atp., dochází k takovým záznamům a jejich změnám, že je vždy kvalita a objektivní výpovědní hodnota zcela subjektivní i u stejných zařízení a technologií, a to u každé konkrétní implementace)

# závěrem

Většina zadavatelů znaleckých posudků, resp. účastníků řízení se domnívá, že jsou dostatečně připraveni na případné vyšetřování, založené na základě stávajícího ICT prostředí a jeho nastavení.

Obvykle je tento předpoklad velmi rychle vyhodnocen jako lichý, a to již v prvotním zhodnocení digitálních stop např. znalcem. Teprve v tento okamžik vzniká konfrontace s objektivním pohledem skutečně průkazných stop (logů, informací), které jsou schopny ustát důkazní břemeno při procesu dokazování.

Zejména se jedná o problematiku ustanovení uživatelů, cyklického přepisu důležitých logů systémů, vlastní práce a prvotní vyšetřování na originále digitálních stop vlastníky, nezaznamenání a nearchivace klíčových událostí systémů, atp.

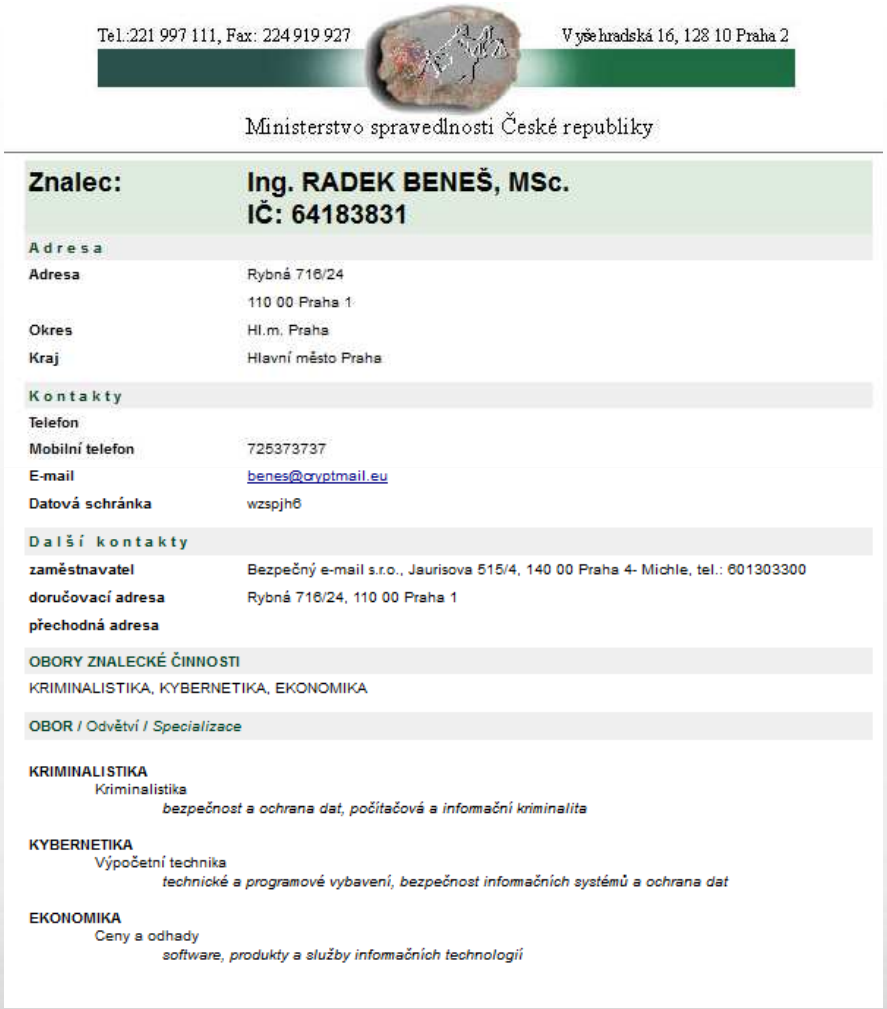
# závěrem

Je kladen důraz nad zamyšlení se nad otázkou, zda jsme schopni hodnověrně a objektivně zodpovědět např. v provozu společnosti otázky: **kdo** (jaký uživatel konkrétně), **co** (s jakými informacemi, software, daty), **kdy** (časová razítka, synchronizace času, vhodné uložení dat, využití služeb třetích stran), **kde** (fyzická lokace, využití konkrétní techniky, umístění dalších stop), **jak** (jak bylo užíváno, bezpečnostní politika a její soulad), **čím** (zda byly připojeny jiná i vzdálená datová úložiště, využita komunikace k přenosu, připojena neautorizovaná technika, provoz na síti), **proč** (stanovení možných předpokladů záměrů útočníků a jejich pravděpodobného postupu, taktika), se může velmi brzo stát nepostradatelnou součástí ICT společností, řízení rizik a bezpečnosti, které poskytnou jistotu společnosti nejen v konkrétních případech vyšetřování, ale uchová i dobré jméno a další cenná aktiva.

# poselství

Nepodceňujme vzrůstající potřebu průkazné informatiky a přenesení těžiště vyšetřování do IT sféry, která je logickým důsledkem naší informační doby, kdy (jako informační společnost) digitalizujeme téměř celé své okolí.

# děkuji za pozornost



Tel.:221 997 111, Fax: 224 919 927 Vyšehradská 16, 128 10 Praha 2

Ministerstvo spravedlnosti České republiky

| | |
|---|---|
| **Znalec:** | **Ing. RADEK BENEŠ, MSc.** |
| | **IČ: 64183831** |
| **Adresa** | |
| **Adresa** | Rybná 716/24 |
| | 110 00 Praha 1 |
| **Okres** | Hl.m. Praha |
| **Kraj** | Hlavní město Praha |
| **Kontakty** | |
| **Telefon** | |
| **Mobilní telefon** | 725373737 |
| **E-mail** | benes@cryptmail.eu |
| **Datová schránka** | wzspjh6 |
| **Další kontakty** | |
| **zaměstnavatel** | Bezpečný e-mail s.r.o., Jaurisova 515/4, 140 00 Praha 4- Michle, tel.: 601303300 |
| **doručovací adresa** | Rybná 716/24, 110 00 Praha 1 |
| **přechodná adresa** | |

**OBORY ZNALECKÉ ČINNOSTI**

KRIMINALISTIKA, KYBERNETIKA, EKONOMIKA

**OBOR** / Odvětví / *Specializace*

**KRIMINALISTIKA**
Kriminalistika
*bezpečnost a ochrana dat, počítačová a informační kriminalita*

**KYBERNETIKA**
Výpočetní technika
*technické a programové vybavení, bezpečnost informačních systémů a ochrana dat*

**EKONOMIKA**
Ceny a odhady
*software, produkty a služby informačních technologií*


**Radek Beneš, znalec v oborech ICT**

benes@cryptmail.eu, +420 725 37 37 37,

www.radek-benes.cz

office@radek-benes.cz, +420 601 303 300


- Kriminalistika
  - bezpečnost a ochrana dat, počítačová a informační kriminalita
- Kybernetika, výpočetní technika
  - technické a programové vybavení, bezpečnost informačních systémů a ochrana dat
- Ekonomika, ceny a odhady
  - software, produkty a služby informačních technologií

http://www.radek-benes.cz

# použité zdroje


Bezpečnost není jen zabezpečení, Computer World 1/2015, Radek Beneš

Veřejná webová prezentace Radek Beneš, http:// www.radek-benes.cz

Statistika PČR a tiskové zprávy z veřejného portálu http:// www.policie.cz

Celosvětový průzkum hospodářské kriminality 2014, poradenská spol. PwC, http://www.pwc.com

Institut pro kriminologii a sociální prevenci, Počítačová kriminalita, Nástin problematiky, Kompendium názorů specialistů, RNDr. Stanislav Musil

Základní definice vztahující se k tématu kybernetické bezpečnosti, veřejný portál MVČR, http://www.mvcr.cz

Hodnocení znaleckého posudku, Prof. JUDr. Jan MUSIL, CSc., Ústavní soud České republiky, http://www.mvcr.cz

Profesionalita znaleckého zkoumání, Ing. Marián Světlík, Digital Forensic Journal 1/2014, http://www.rac.cz

Vyhledávání a zajišťování kriminalistických stop na místě činu, prof. JUDr. Ing. Viktor Porada, DrSc., Ing. Jaroslav Suchánek, CSc., prof. PhDr. Jiří Straus, DrSc., Policejní akademie ČR Praha

Digitální stopy v kriminalistice a forenzních vědách, Doc. Ing. Roman Rak, Ph.D., Prof. JUDr. Ing. Viktor Porada, DrSc., dr.h.c, Policejní akademie ČR Praha

Počítačová kriminalita a bezpečnost, Miloslav Macháček, http://www.internetprovsechny.cz

SMEJKAL, V.,SOKOL, T.,VLČEK, M. Počítačové právo. Praha, C. H. Beck/SEVT 1995