MUNI
LAW

Integrita elektronického důkazu: technické a organizační postupy

Jakub HARAŠTA

MUNI
LAW

Obecně k integritě

Integrita důkazu

- Legalita – důkazní prostředky získané legálně
- Integrita – prevence změny při úkonech
- Opakovatelnost/přezkoumatelnost – metody
- Nepodjatost – nestrannost osoby provádějící analýzu

- Přípustnost důkazu

Integrita důkazu II

- Ke spolehlivému zjištění skutkového stavu je nezbytné, aby byl důkazní prostředek opatřen a přechováván způsobem, o němž nejsou pochybnosti, že mohl být jakkoliv, úmyslně, z nedbalosti nebo pouhou náhodou, upraven, pozměněn nebo změněn za prostředek jiný.

  (ÚS ze dne 15.2.2016, sp. zn. I.ÚS 368/15)

Integrita důkazu III

- Pokud při provádění a hodnocení důkazů vyvstanou vážné pochybnosti o spolehlivosti použitých důkazních prostředků, o něž se opírá důkaz viny obžalovaného ze stíhaného skutku, je povinností soudu se s nimi spolehlivě a přesvědčivě vypořádat.

  (ÚS ze dne 15.2.2016, sp. zn. I.ÚS 368/15)

Různé úrovně

- Interní vyšetřování
- Civilní řízení
- Trestní řízení

- Účel: důkazy, které mají být využity/prezentovány nebylo možné pozměnit (šance byla minimalizována)

Interní vyšetřování (kybernetický incident)

- Chceme rychle dosáhnout plné funkčnosti?
- Chceme opatřit důkazy?
- Buď… anebo…

MUNI
LAW

Technická opatření

Technické postupy

- Extrakce dat
- Bitová kopie dat
- Kontrolní součet dat

Bitová kopie

- Zavedeno v 90. letech Kriminalistickým ústavem PČR (forenzní kopie dat disku). Jeden z pilířů zajišťování digitálních stop.

- Nedochází k manipulaci s originálem (resp. manipulace s originálem se minimalizuje)

Bitová kopie II

- Kontrolní součet jako důkaz, že nedošlo k porušení integrity (originál vs. kopie)
- Různé algoritmy (MD5, SHA1, SHA256…)

- Obraz disku + otisk disku pro autentizaci digitálních stop
- Zabalení a zapečetění objektů obsahujících digitální stopy

Bitová kopie III

- Ne vždy se vytváří otisk všech souborů jednotlivě
- RAR archiv

Bitová kopie IV

- Hodnota kontrolního součtu se uvádí do protokolu
  - Co když to nejde?

Digitální vs. materiální

- Data NEBO nosič (autentizace jako u materiální stopy)

- Nepřepisovatelné médium (CD/DVD) označené číslem jednacím, podpisem zajištěné osoby (+ nezúčastněná) přímo na médium (autentizace podpisem)

Problém „živých“ dat

- Je to problém?
  - Forenzní postupy vs. právní otázky

MUNI
LAW

Organizační opatření

Protokolace

- CO je důkazem?
- JAK se vyšetřovatelé k důkazu dostali, jakým způsobem byl opatřen?
- KDY byl důkaz získán a kdy použit?
- KDO s důkazem pracoval a měl k němu přístup?
- PROČ s důkazem osoba pracovala?
- KDE se důkaz nacházel a jak se mezi různými místy pohyboval?

Protokolace II

- Předání mezi osobami/orgány
- Časová posloupnost jako neporušená a zdokumentovaná časová řada

§88 odst. 6 TŘ

- *„Má-li být záznam telekomunikačního provozu užit jako důkaz, je třeba k němu připojit protokol s uvedením údajů o místě, času, způsobu a obsahu provedeného záznamu, jakož i o orgánu, který záznam pořídil.“*

MUNI
LAW

Integrita jako předmět diskuze

Je to problém?

- Není to problém, dokud to není problém.
- Většina záležitostí projde bez povšimnutí, dokud není rozporována – technické minimum pro právníky?
- OČTŘ často v těchto postupech nemají jasno nebo je nedostatečným způsobem vynucují!

UK ACPO Guidelines

- P1: Žádná akce vyšetřujícího orgánu nesmí změnit data, u kterých ze očekávat, že se na ně bude spoléhat soud.
- P2: Když je nezbytné přistoupit k originálním datům, musí tak činit kompetentní osoba schopná vysvětlit důvody a implikace.
- P3: Audit trail musí být vytvořen a zachován. Nezávislá třetí strana musí být schopná postupy prověřit a dosáhnout téhož výsledku.
- P4: Osoba vedoucí vyšetřování má celkovou zodpovědnost za dodržování práv a postupů/doporučení.

Po čem pátrat?

- Jak byla vytvořena bitová kopie a kdo ji vytvořil?
  - Nástroj, kvalifikace
- Jakým způsobem byla využitá prázdná datová úložiště připravena?
  - Forenzní sterilita
- Byl obal k uchování materiální stopy porušen? Kdy, jak, proč? Jak je toto zadokumentováno?
  - Podpis přes pečeť, video dokumentace porušení pečeti a následných úkonů apod.

Po čem pátrat? II

- Jakým způsobem byl důkazní materiál předán znalci?
  - Zapečetěný obal vs. neuzavřená igelitka Billa
- Došlo k přelepení mechanik, aby nemohly být využity? Došlo k označení portů apod.?
- Existuje na nosiči soubor se systémovým časem po datu zabavení věci?