MUNI
LAW

Kyberkriminalita (stíhání a dokazování)

Václav Stupka

Hlavní témata

- Specifika stíhání kyberkriminality
- Institucionální zajištění
- Postupy při vyšetřování kyberkriminality
- Elektronické dokazování kyberkriminality

MUNI LAW

Specifické požadavky

- Znalost technologií, specifického práva, mezinárodních souvislostí
- Předpokládá se širší spolupráce s podpůrnými orgány PČR
- Kvalifikovaný personál
- Technické vybavení
- Spolupráce s průmyslem a akademickou sférou
- Specifické požadavky jak na úrovni PČR, tak i SZ a soudů

- > Důležité je budování kapacit

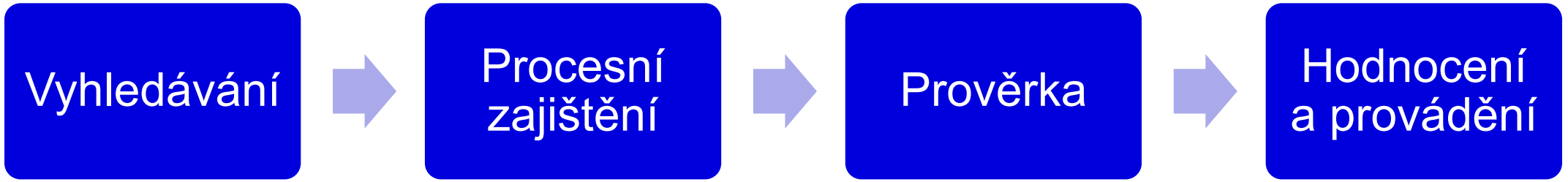
Specifické orgány a jejich rozvoj

- Policie:
  - Specializovaná pracoviště na KŘ
  - Odbor kriminalistické techniky a expertíz (OKTE)
  - Oddělení počítačové expertizy – Kriminalistický ústav Praha
  - Útvar zvláštních činností Policie ČR (ÚZČ)
  - Národní centrála proti terorismu, extremismu a kybernetické kriminalitě (NCTEKK)
- Státní zastupitelství:
  - Síť kyberspecialistů
- Soudy
- Další OVM
- Znalci, odborná veřejnost

Specifické postupy

MUNI LAW

Fáze procesu dokazování



MUNI LAW

Různé zdroje důkazů a specifika jejich zajišťování

- Trestní řád neobsahuje výslovnou úpravu, a je tedy třeba k zajišťování elektronických důkazních prostředků často využívat nepříliš vhodné procesní nástroje
- K počítačovým datům se lze dostat v zásadě třemi základními způsoby:
  - Zajištění zařízení či datových nosičů (hardware)
  - Přímý přístup k datům (lokální\vzdálený)
  - Přístup prostřednictvím držitele/správce dat

MUNI
LAW

Díky za pozornost

stupka@muni.cz