# Počítačová kriminalita
# současný stav a vývojové tendence

Doc. JUDr. Josef Kuchta, CSc
KTP PrF MU Brno

- Počítačová kriminalita – závažný fenomén u nás i v celosvětovém rámci.
- Neustálý technický a technologický rozvoj
- Značné škody
- Nebezpečí do budoucna
- Nedostatečná právní úprava
- Základ : Budapešťská úmluva z roku 2001
- Úmluva Rady Evropy z roku 2005

- Ke změnám dochází a bude docházet zejména v těchto oblastech :
- Změna terminologického názvosloví a upřesnění pojmu
- Nové specifické podoby jednání a formy provedení
- Změny a rozšíření jurisdikce států ke stíhání
- Změna charakteristik pachatelů

- Dopady zavedení trestní odpovědnosti právnických osob
- Změna způsobu vedení vyšetřování a dokazování
- Nutnost legislativních úprav
- Zavádění nových způsobů trestání
- Nové způsoby prevence včetně kybernetické bezpečnosti

- Počítačová kriminalita
- Kybernetická kriminalita
- Internetová kriminalita
- Informační kriminalita
- Informatická kriminalita
- E-kriminalita
- Každý z těchto pojmů má svůj význam

- Charakteristika počítačové kriminality:
- Vysoká diskretnost a latence
- Značné škody
- Specifika pachatelů – různé vrstvy, různé motivy
- Složité způsoby odhalování a dokazování
- Zvýšený podíl organizovaných pachatelů
- Mezinárodní charakter

- Nedostatek boje s touto trestnou činností
- Subjekty prevence – v první řadě oběti, ale i stát v případě napadení veřejných zájmů
- Snadno dostupné prostředky páchání
- Tolerance, případně i uznání společností
- Nedostatečné právní vědomí pachatelů i společnosti

- Aktuální typy útoků:
- Nigerijský spam, phishing, ransomware, adware, spyware, trojský kůň, logical bombs, pharming crimeware, hacking, cracking, spoofing, phreaking,cybersquatting, carding, skimming, hoax, backdoor útok, keylogger, defacement
- DDoS – Distributed denial of service

- Změněné způsoby provádění klasické TČ:
- Kybergrooming,
- Kyberstalking,
- Kyberšikana,
- Happy slapping
- Kybermobbing
- kyberterorismus

- Pachatelé :
- Nejprve psychologické motivy, odpovídající charakteristice počítačů a internetu
- Nyní motivy zištné, ideologické, teroristické
- Poměr muži – ženy
- U nás nedostatečně propracované charakteristiky – vzor u zahraničních výzkumů – např. americké výzkum y u stalkingu

- Prevence :
- Ve vztahu k potencionálním pachatelům a obětem – výchova
- Technické zabránění pachatelům – ochrana počítačů, zabránění v přístupu
- Legislativa

- Represe :
- Trestněprávní úprava v TrZ
- Rozšíření trestnosti právnických osob
- Nové způsoby zacházení s pachateli – trest zákazu práce s internetem
- Nová úprava v trestním řádu, resp. v zákoně o mezinárodní justiční spolupráci
- Organizace orgánů činných v trestním řízení

- Kybernetická bezpečnost.
- Úkol státu zabraňovat závažným napadením, ochrana před napadením významných informačních systémů a kritické iánformační struktury.
- Zákon č. 181/2014 Sb. s prováděcími vyhláškami
- Návrhy- omezení přístupu k internetu

- Další směry vývoje počítačové kriminality.
- Objektem útoku převážně informace
- Mobilní zařízení jako nástroj útoku
- Rozšíření útoků proti kybernetické bezpečnosti
- Cílevědomé útoky soukromých skupin
- Masívní šíření nepravdivých údajů
- Prohlubování střetu mezi ochranou soukromí a požadavky na bezpečnost.

- Blíže viz např. nejnověji :
- Smejkal,V.  Kybernetická kriminalita, Plzeň: Aleš Čeněk, 2015
- Dále např. publikace vydávané speciálním Ústavem počítačových technologií na Právnické fakultě v Brně.

- Děkuji za pozornost