Abstrakt

Předmětem této diplomové práce je šíření ransomware, které je aktuálně jednou z nejzásadnějších globálních kybernetických hrozeb. Ransomware je škodlivý kód, který při své aktivaci v počítačovém systému zpravidla zablokuje přístup k tomuto systému či zašifruje data v něm obsažená, na základě čehož poté uživatele vydírá. Tato práce se zabývá kriminologickými a trestněprávními aspekty tohoto fenoménu.

Ve své kriminologické části se tato práce zabývá otázkou etiologie šíření ransomware a kriminogenními faktory, přičemž mimo jiné zkoumá aplikovatelnost kyberkriminologické teorie *space transition theory* na daný fenomén. Dále se zabývá viktimologickým aspektem věci, přičemž vyjmenovává nejzásadnější faktory ovlivňující viktimizaci, a to jak v případě plošných nezacílených ransomware útoků, tak v případě útoků konkrétně zacílených. Rovněž zkoumá otázku vysoké latence tohoto fenoménu a kyberkriminality obecně a možnosti prevence, kterou hodnotí jako nejlepší způsob obrany proti ransomware útoku. Zvlášť se zabývá otázkou ransomware útoků na nemocnice a kritickou infrastrukturu, otevírá rovněž téma nárustu počtu útoků v důsledku pandemie COVID-19. Obsažena je i problematika politicky motivovaných kybernetických útoků. V závěru kriminologické části je uvedena prognóza budoucího vývoje, ne příliš optimistická.

Ve své trestněprávní části se tato práce zabývá především právní kvalifikací šíření ransomware z pohledu českého trestního práva hmotného. Ojedinělá je tato práce v tom aspektu, že se zabývá trestněprávní kvalifikací šíření ransomware s ohledem na různé druhy ransomware, jako je šifrovací ransomware, locker ransomware či policejní virus. Následuje kritické zhodnocení současné právní úpravy trestní odpovědnosti za tento typ kriminálního chování a závěrem je představen konkrétní návrh *de lege ferenda*.