Criminological and legal aspects of the ransomware phenomenon

Abstract

This diploma thesis deals with the current topic of cybercrime and focuses specifically on the phenomenon of ransomware on a scope unprecedented in Czech legal literature. Ransomware is a malicious code that interferes with the operation of a computer system, and later requires ransom for the victim to recover the access to the computer system and the data contained therein. Basic concepts necessary for the definition of ransomware (such as cyberspace, cybercrime, computer system, malicious code, cryptocurrency and darknet) are introduced and explained. The specificities of cybercrime and its development and current range in the Czech Republic are analysed.

The main part of the text deals with the analysis of ransomware, starting with its history and leading to the possible future developments of ransomware. Different variants of ransomware are described such as false antivirus, police, locker and encryption ransomware. From a criminological point of view, the text focuses on the unique interaction of the perpetrator and the victim, which takes on surprising forms of customer support, answers to frequently asked questions and instructions for acquiring virtual currencies. Emphasis is placed on prevention efforts that can mitigate the damage of the ransomware attack itself. The burning question of whether to pay the ransom is also addressed.

In the final part of the thesis, the emphasis shifts to the criminal law implications of the ransomware attack under the current legal system in the Czech Republic. Ransomware may be sanctioned as fraud, extortion, false personation or unauthorized access to the computer system, depending on the circumstances of the attack. Concurrence of some of these offenses is very likely in such cases. The text also assesses the quality of the current legal regulation of cybercrime in the Czech Republic and answers to its most frequent criticism.

Key words: ransomware, cybercrime, malware