Criminal and criminological aspects of ransomware spreading

Abstract

This diploma thesis deals with issues of ransomware spreading and examines certain criminal and criminological aspects of this cybercrime phenomenon. Ransomware is malware that encrypts, blocks or prevents access to the computer system or data in a computer system. In connection to this, it demands monetary or other ransom. This diploma thesis firstly describes ransomware from the point of view of its function and technical aspects, including its history, categorization of its variations and description of several notable infection examples, namely WannaCry, Petya, DoubleLocker and Vir Policie.

Following section describes possible criminal qualifications according to Czech substantive criminal law, including the consideration of specifics of different ransomware variations and potential development of this criminal aktivity.

The final part focuses on criminological aspects of ransomware spreading. It beggins with a description of the crime status and dynamics, including further details about latency and trends. Then follows the description of perpetrator and victim in view of certain criminological theories. Finally, criminological part comprises a chapter about crime control and prevention, which includes practical parts that aim to help with practical prevention.

Key words

ransomware, malware, computer crime, cybercrime