Abstract

The subject of this diploma thesis is the ransomware spread, which is currently one of the most prominent global cybernetic threats. Ransomware is malicious code that, when activated on a computer system, usually blocks access to that system or encrypts the data contained in it, which is then used to blackmail the user. This thesis deals with criminological and criminal aspects of this phenomenon.

In its criminological part, this thesis deals with the issue of the etiology of the ransomware spread and its criminogenic factors, while examining, among other things, the applicability of cybercriminological theory named *space transition theory* to a given phenomenon. It also deals with the victimological aspect of the matter, listing the most fundamental factors influencing victimization, both in the case of widespread non-targeted ransomware attacks and in the case of specifically targeted attacks. It also examines the issue of the high latency of this phenomenon and cybercrime in general and the possibility of prevention, which it considers to be the best way to defend against a ransomware attack. In particular, it deals with the issue of ransomware attacks on hospitals and critical infrastructure, and also raises the issue of the increase in the number of attacks due to the COVID-19 pandemic. The issue of politically motivated cyber attacks is also included. At the end of the criminological part, the prognosis of future development is given, not very optimistic.

In its criminal law part, this work deals mainly with the legal qualification of the spread of ransomware from the perspective of Czech substantive criminal law. This work is unique in that manner, that it deals with the criminal qualification of the ransomware spread with respect to various types of ransomware, such as crypto ransomware, locker ransomware or police virus. Critical evaluation of the current legislation of criminal liability for this type of criminal behavior follows, and in conclusion, a specific proposal *de lege ferenda* is presented.