26.05.2023

Ransomware in Switzerland

The Nationale Zentrum für Cybersicherheit (NCSC) mentions ransomware reports in their half-yearly 2022/II 76 report. About one third concerns private individuals, two thirds companies. As far as attacks on companies are concerned, the most active ransomware there is “Lockbit”; for private individuals it is mainly “Deadbolt”.

A ransomware attack involves the encryption of data and a ransom demand, frequently demanded in a cryptocurrency. Many companies have recognised this threat and have recently adapted their back-up strategies. Simply encrypting data is therefore no longer lucrative enough for most attackers; something which motivates them to carry out so-called double and triple extortions. In addition to encrypting data, they will also then threaten to publish them. With cases of triple extortion, customers and suppliers are also blackmailed, threatening them with the encrypted data and their publication.

An NCSC report dated 22nd May warns that ransomware gangs are still very active in Switzerland. Several companies went public last week, confirming that criminals carried out successful ransomware attacks on them and that data were encrypted. It is therefore of particular importance to always keep systems up-to-date and adequately protect access to them.

Further information on ransomware can be found here (https://www.ebas.ch/en/ransomware-encryption-trojans/) .

You can read the complete NCSC report on ransomware gangs in Switzerland here (https://www.ncsc.admin.ch/ncsc/en/home/aktuell/im-fokus/2023/ransomware-2023.html) .