DRACOON

Date: *June 01, 2019*
Source: *EHZ Austria*
https://www.dracoon.com/wp-content/uploads/2019/06/2019-06-01-EHZ-Austria-Statement-Ransomware.pdf

Press Report

Ransomware

Never-ending

A comment by Marc Schieder, CIO DRACOON:

“Once again, the German Federal Office for Information Security (BSI) urgently warns of attacks resulting in the execution of an encryption trojan. The shocking part: This time cyber criminals are using methods only known to the intelligence agencies until a few months ago, according to the federal office. To first access the respective company network the so-called dynamite-phishing in form of large-scale spam-campaigns is often used as a first step. As soon as the attackers have infiltrated the network they can spread further. Here, the criminals try to manipulate or delete possible backups. Finally, they infect the computer systems of promising targets coordinated with ransomware that is executed eventually.

The question of how companies can protect themselves against such attacks, can be answered both technically and organizationally. Regarding the IT-environment in companies there are certain criteria to look out for when implementing new solutions, e.g. in the field of filesharing, such as an integrated ransomware protection. Here for example, encrypted data can be quickly restored from the paper basket in case of an attack, as all reversion information is stored. This works as follows: In case of a ransomware attack the data with encrypted information is overwritten – their unencrypted versions on the other hand are automatically saved to the paper basket and can be restored completely and unharmed. In an attack-situation the technology prevents a massive data loss that could cause critical harm to the company.”

www.dracoon.com