DRACOON

Date: *March 29, 2019*
Source: *av-finance.de*
http://www.av-finance.com/geldinstitute/newsdetails-gi/artikel/334/ransomware-die-nicht-endende-gefahr/

Press Report

Ransomware: the never-ending danger – BSI warns of new attack methods

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 most 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. This method is already known in connection with the Trojan Emotet that, for years, has been responsible for millions in damage in German and international companies. 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 resulting operation malfunctions are substantial, and the ransom demands considerably higher compared to earlier ransomware attacks.

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.

On an organizational level it is important to sufficiently inform and train employees in all departments about current hazards. It is especially important – as the BSI also emphasizes in its statement – to take the danger seriously and be prepared. President Arne Schönbohm states clearly that IT-security should be seen as a prerequisite for digitization in order to profit from this development permanently. As a German Enterprise-Filesharing Solution we addressed the IT security challenges of digitization early on, and privacy and data security have been top priorities since day one. Only if the developers of IT security solutions assume their responsibility and at the same businesses of all sectors take the threats to cyber

security seriously can the danger be averted. Software as well as the organizations that use it need to urgently keep up with degree of professionalization of the hackers. This way, Germany as a business location is protected from massive financial losses, and even sophisticated methods of attack ultimately run nowhere.