DRACOON

Date: *October 30, 2018*
Source: *ITSecCity.de*
http://www.itseccity.de/markt/kommentare-meinungen/dracoon151118.html

Press Report

Cyber Security in times of Digitalisation

Ongoing high-risk potential caused by ransomware
Security by default enables even inexperienced users to work with a system configuration that effectively protects their data while using IT systems

A comment by Dr. Florian Scheuer, CTO from Dracoon

The BSI-president Arne Schönbohm and minister of the interior Horst Seehofer presented the latest federal status report. According to this report, the absolute numbers of threats and attacks have risen in all sectors over the last few years. This is not surprising considering the advancing digitisation of agencies and enterprises on the one hand. On the other hand, the detection of IT-security incidents is bound to grow through higher awareness in the companies and reporting obligations. Unfortunately, the report does not contain any findings concerning the dark figure of successful attacks. Furthermore, throughout the report there is a continuous blending of numbers between the detected, repelled attacks and the successful (detected) attacks. This makes it difficult to interpret the data of the report.

Nevertheless, the report shows that ransomware – even though it's largely vanished from media reports – is still a big threat that causes considerable damage. Especially the ongoing split-up of malware makes a reliable detection ransomware ever more difficult. That is why accompanying measures that enable a recovery of the encrypted data are essential.

In conclusion of the report the BSI emphasises that – given the threatening situation -the cyber security in digitisation has to be taken more strongly into account. In particular, the federal agency calls for the use of systems in the administration, economy and among private users, which were developed according to the principle of "security by design" and "security by default".

For systems designed with "security by design" in mind, security features have been deeply conceptualized early in their development. It often turns out, for that for example retrofitting effective client-side encryption for the effective protection of information is not easy and sometimes leads to a deterioration in usability – the most prominent example of this is probably e-mail encryption. In addition, "security by default" ensures that even inexperienced users operate with a system configuration that guarantees them and their data effective protection when using IT systems. Therefore, these two aspects counteract high economic, but also idealistic damage.

It is unfortunate that the BSI makes no reference to the trade in security holes, which continues to be carried out by various German authorities and thus does not clearly position itself against this practice. Acting on the existing – and thus state-supported – market for vulnerabilities threatens the security of German companies and authorities massively, as the there offered and acquired security vulnerabilities usually exist in a variety of currently used systems and are not reported to the affected manufacturers for elimination. There is no assurance that these security holes will not be sold to or discovered by other actors.

Nevertheless, the BSI report shows especially one thing in particular: The growing threat situation in the sector of IT-security in Germany should be taken as an occasion by the companies and IT-manufacturers to check their solutions for data security and to make necessary arrangements. Hereby a data protection-friendly technology design as well as a privacy-friendly pre-setting, which a software should already consider during its development, play a decisive role.