The story behind CySCoS

Malicious software and the consequences of its execution in data processing systems cost resources. In the case of ransomware, this can be immediate monetary value. More often - and in the case of ransomware, additionally - economic damage occurs through system failures and the time and support required to eliminate the indirect and immediate consequences.

The names of malicious programs are regularly mentioned in the press as the culprits, but they are not the only ones to blame. Errors or so-called weak points in utility programs are also cited. This inevitably leads to calls for regular updates and for users to be vigilant.

The real reason for the success of malware lies in the inadequacy of the hardware currently used! In fact, hardware can do what software cannot in principle: recognize malware as such without using static or dynamic attributes to help.

There are three main reasons that pave the way for malware - and they can easily be proven in concrete installations:
1. Data and programs are exchanged over the same physical interfaces.
2. Data and programs are stored without physical separation, in both main memory and permanent storage.
3. Data processing and program management are carried out by the same processors.

These three deficiencies in hardware design were identified and published after the successful attack on RSA (March 2011). In order to bring about a significant improvement at this point, this alternative hardware architecture was designed. The greater security is achieved by the fact that
- there are mutually incompatible interfaces for data and programs,
- there are several physically independent memory components to which the individual data structures are allocated separately,
- in addition to the main processor, which is intended for data processing, there is a so-called load processor, which is responsible for loading and managing programs.

These precautions make the architecture incapable of executing malware.
Once the separation of data and instructions has been achieved in order to increase security, then this hardware architecture suggests further development potential, such as a significant increase in the bandwidth for data transfers between processors and storage units. This would serve projects such as big data, artificial intelligence or efficient and secure data transmission between networks with different access attributes.

A demonstrator of this architecture is available.