DRACOON

Date: *April 05, 2019*
Source: *sysbus.eu*
https://www.sysbus.eu/?p=14153

Press Report

Authority 4.0: the importance of cloud storage and the GDPR

Author/Editor: Marc Schieder, CIO DRACOON (https://www.dracoon.com/de/)

In the wake of the growing digitalisation of analogue data, organisations in the public sector are being confronted with new challenges – however, they are also connected to new possibilities. With the growing use of mobile devices and the constant and immediate availability of data, which is often taken for granted, the user-behaviour changes and therefore also the expectations of the citizens and the economy. To meet these expectations, new needs and requirements must also be responded to in the government environment. At the same time organizations in the public sector are increasingly experiencing efficiency pressure.

Picture: DRACOON

Old processes are no longer safe

For a long time, organisations in this sector have been reluctant to answer the question of outsourcing IT to the cloud (https://www.sysbus.eu/?cat=22). Even though, choosing the right solution increases the efficiency and data security. Especially the model of the hybrid-cloud combines many advantages for the public sector. Hybrid means, there is a central operation, but dedicated technologies or resources of the authorities or municipalities can be operated optionally and additionally on site or in an own data centre – such as storage (https://www.sysbus.eu/?cat=17), identity or key management in the field of encryption.

Within the public sector, however, there is sometimes still the unfortunate idea that it would be best and safest to do without the cloud and exchange data internally via e-mail or file servers, as has been the case in the past. However, a number of reasons show that this is not advisable. Existing silo-structures need to be eliminated – they are neither manageable nor securable. A central service on the other hand, offers great advantages. In this context, more security is also provided by the additional activation of a Security (https://www.sysbus.eu/?cat=37) Operations Centre (SOC), in which all attack vectors are centrally filtered out. In addition, there is a central malware scan that docks to SIEM systems, allowing attack vectors to be mitigated. A central software-service model with a hybrid-concept, allowing the organisation to keep their sovereignty over certain components, offers an economical and secure thought-out operating model.