CENTRALISED PROCESSES IMPROVE IT SECURITY

The digital transformation keeps changing our life at an extremely fast pace and has made it more comfortable in many facets. The expectations and demands on IT-enabled processes in the tank storage business has increased significantly over the last few years.

Due to the growing complexity of the hardware and software systems coupled with increasing connectivity and integration, the demands on the security and supervision of IT systems are growing disproportionately.

The outsourcing of IT systems for dispatch handling and inventory management to an external service partner is a reasonable and efficient way of dealing with the new challenges. Not only do you avoid cost-intensive trainings of personnel and investments in new hardware – it also ensures an increased level of data security within a fixed budget.

For example, fast internet-based communication technologies used for connecting different integrated inventory control systems or for the clearing of electronic customs procedures have become standard systems for storage tanks.

EMCS and PIDX are two widely known specifications of this ongoing development. Further applications are being developed and will continue to present storage operators with new challenges.

EXTERNAL SERVICE PARTNERS INSTEAD OF LOCAL DESKTOP SERVERS

Dispatch and storage handling need flexible and scalable processes in order to generate the required performance and improvement in efficiency.

Operators of tank facilities could well think that the increasing digitalisation and integration of processes could put their systems at risk of losing confidentiality, availability and system integrity.

Currently, many dispatch and inventory management systems are still run via local desktop servers at the tank facilities. Dispatch department staff are responsible for the daily back-up as well as the execution of important security updates. The daily update of systems is becoming even more important and a significant relief is the transition of the in-house system maintenance to an external service partner.

This way, the responsibility of the IT operation is transferred to a professional service partner. As a result, operators can focus on their core competence.

Highly available networks form the basis of outsourcing concepts and the possible centralisation of services. They enable a reliable, data-specific connection to remote locations. It is this method that unites decentralised hardware and software solutions that are allotted to different locations. This simplifies the homogenisation of processes and additionally eases the modernisation of applications for the whole facility.

Outsourcing these systems to an external service partner allows operators to release capacities and increase their capability to act.

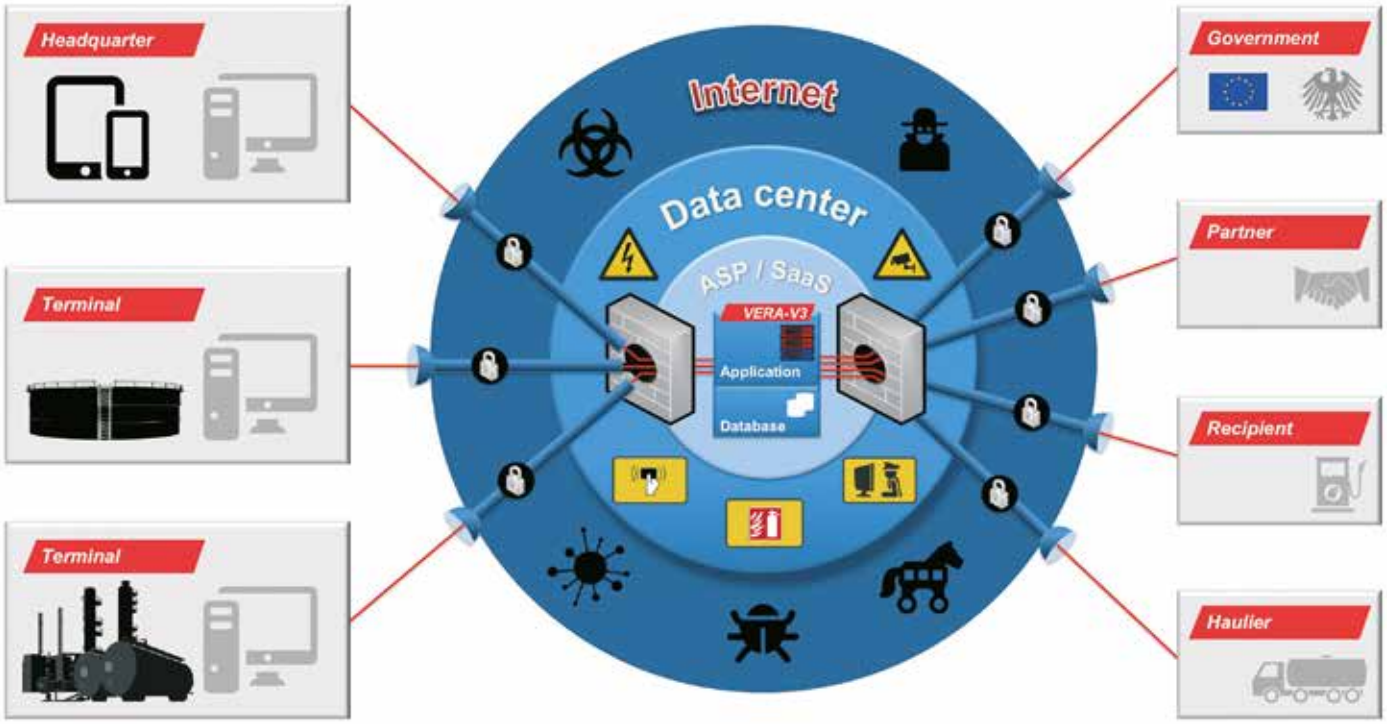
There is a choice between two different options. Either to run systems on dedicated servers at the chosen service partner (ASP – Application Service Provider) or use shared services (Saas – Software as a Service). Both options mean a significant cost reduction, especially SaaS, compared to a local environment.

MORE SECURITY FOR TANK SERVICES

Those who provide these external services are required to meet safety-related requirements, such as the treatment of sensitive and confidential data from the dispatch and

01 Highly available server in a data centre

02 Scheme of a centralised architecture using the example of VERA-V3



02

inventory management systems. The same applies to the protection of the data availability.

In the case of a disruption to an IT component or to the network, the chosen partner has to ensure a high end-to-end availability of the systems. In case of a technical breakdown, the partner has to quickly restore the operational efficiency as well as the highest possible security of information in terms of accessibility, confidentiality and integrity.

This means efficient protection against a loss of information, data theft and manipulation. Adequate solutions are also needed in relation to the visibility, auditability, checkability and flexibility of the data.

In terms of improving IT security there are withfail-proof computer systems with redundant hardware and stringent control mechanisms. A secured infrastructure should also be provided, which ensures a reliable allocation of all services and data from emergency supply over air conditioning and redundant broadband internet access through to the protection against fire and water. Confidentiality is guaranteed by using the latest encryption and firewall technologies for the data transfer and by suitable access controls.

CRUCIAL PROCESSES

In addition to comprehensive technical measures, compliance with stringent maintenance and development processes are also of great importance.

Therefore, it will be helpful to reference widely acknowledged IT-security norms, such as ISO/IEC 27001. These require a distinct allocation of duties and the clear assignment of responsibilities. The maintenance guidelines should describe the processes needed for the daily maintenance of systems. These include the user administration, emergency changes, control, data protection and surveillance of the systems. Within these processes all relevant system levels such as the network, application, database technical breakdown and operation system level should be taken into account. Regular 'disaster recovery tests' should also be included. These are data recovery tests to prove that the whole system could be restored within a few hours and that the system can be restarted at another location if there is a technical breakdown of the whole computing centre.

A development guideline is equally important for the provided software. With this guideline, the service partner fixes regulations and principles for a professional and, as far as possible, trouble-free development process. A transparent and controlled change management is a major pillar of such a development guideline.

Security requirements, risk evaluations, archiving, release administration and test requirements are being fixed within these guidelines. It is advantageous if the chosen provider offers developers, testers and decision makers 'change management tools' to administer and document transparently the process of every single change and software release.

The engagement of highly-qualified personnel should be a matter of course for the chosen provider as well as compliance with processes. A support hotline for the complete life-cycle of the tank storage operation should be available.

TRANSPARENCY AND TRUST ARE ESSENTIAL

Many companies already recognise the opportunity to increase their security through the outsourcing of their systems to a reliable service partner. The centralisation of systems enables stringent control and the allocation of an elaborately secured infrastructure. When considering a service partner it is important to remember to establish a long-term and reliable business relationship and handling extremely sensitive corporate data. Against this background, mutual trust and transparency are essential.

Additionally, audits which include the disclosure of computing environments as well as the description of processes for the maintenance of systems and documentation of compliance is equally important. The date of the last test for the recovery of the system and the duration of the test should also be considered.

Once an agreement with a service partner has been formed it is important to keep up-to-date with their compliance with security regulations. In addition to regular audits, recognised accreditation bodies could provide the respective certifications (e.g. ISO /IEC 27001). A tank farm operator should contractually safeguard guaranteed access to their data in the beginning, in case the cooperation finishes.

The physical storage of the data also needs to be sorted, as the international saving of data might result in the different legal frameworks conflicting.

The centralised outsourcing of major IT systems such as dispatch handling and the inventory management bears huge potential for tank farm operators. It is a significant opportunity to improve processes. Information security depends on the organisational and safety-related level of the chosen service partner. Therefore, it pays to check the performance and competence of any potential partner in advance.

FOR MORE INFORMATION:

Dipl.-Ing. (FH) Johannes Kuhlmann, head of terminal automation department, +49 209 9515 471, kuhlmann@vta.de, www.vta.de