TÜV®

Datum
November, 29th 2013

Strengthening competence and neutrality for cyber security inspections in the EU

VdTÜV (The Association of TÜVs - Verband der TÜV e.V.) supports the proposed EU Directive regarding measures to guarantee a high level of common network and information security in the Union[1]. With the Directive, Europe is setting a legal framework for greater cooperation and more voluntary initiatives in the area of cyber security. In addition, the population of the EU should receive more information about the dangers in cyberspace, aimed at creating greater awareness. VdTÜV e.V. calls upon the EU Commission to create and structure long-term measures for strengthening IT and cyber security in Europe by means of a *Roadmap for IT-Security.*

Ongoing development and use of modern information and communication technologies is essential for European prosperity. Increasing digitisation of value added chains in the different sectors, such as transport, energy, health and finance, is raising their growth potential. At the same time, the critical infrastructures of these sectors must be safeguarded against threats in order to protect the common good and ensure national and European sovereignty and independence. Companies and organisations with critical infrastructures, and also important state authorities, should strengthen the resistance of their own processes and the information and communication technology they use against cyber attack.

In particular, this involves increasing internal cyber security competence by creating suitable structures in the companies and public authorities and providing sufficient training for employees so that they have the necessary skills and expertise. We recommend the use of established safety standards, such as for example ISO/IEC 27001 ff., the internationally valid Common Criteria and best practice approaches such as OWASP, which have been successfully addressing the above themes for many years.

In addition, special considerations and industrial IT Security Standards and Norms (Industry 4.0) must be developed further or at least harmonised. Adequate standards are necessary in order to achieve reliable high security levels in companies and public authorities. In addition, regular auditing of the security structures by independent, accredited experts should be specified for companies and state organisations who are considered critical with regard to the common good.

The EU Draft Directive only offers a vague description of the requirements and necessary competences of the independent bodies who will be commissioned with cyber security audits of market participants and public administration bodies. However, these independent bodies should have the same competences throughout the EU to qualify them to perform all kind of inspections and certifications. The sovereign accreditation[2] of independently notified conformity assessment bodies is a guarantee of reliability, credibility and trust in the case of certification procedures based on relevant legal acts, measures and standards.

[1] See EU Commission Proposal KOM(2013)48 final

[2] Compare: Regulation(EC) No. 765/2008 setting out the requirements for accreditation and market surveillance