Verband der TÜV e.V.

TÜV®

Date
22-Feb-18

VdTÜV position on the regulation proposal for a European "Cybersecurity Act" from 13 September 2017

Ten recommendations for a sound European "Cybersecurity Act":

1. VdTÜV welcomes that the requirements for the conformity assessment bodies comply with the "New Legislative Framework". In order to guarantee quality and confidence, only accredited third-party bodies shall be authorised for conformity assessment and certification. The interplay of independent conformity assessment, accreditation, notification, and national market surveillance provides effective and sustainable consumer protection.
2. The trustworthiness of a certificate is dependent on the assessment by an independent third-party body. Higher-risk products, services, processes, and systems must be subject to a mandatory assessment.
3. The certification must always merit the highest possible trust. It should be definitive, reliable, and transparent. A certification must always consider the risk of a product or service through depth and quality of the assessment. The higher the risk, the more comprehensive the assessment must be.
4. Since important functions are no longer components of the IoT product ("backend" systems), assessments must go beyond a limited product perspective.
5. The specification of responsibilities needs to be clarified. Who assesses and certifies, who notifies and who accredits must be clearly defined. To avoid conflicts of interests, the various actors may only be responsible for one single role at a time. Exceptions must be clearly defined and limited.
6. A label must be described specifically and consistently. It must provide a risk-adequate promise of security. Certification and awarding of labels require that an accredited third party carry out the assessment. The name of the responsible independent third party should be included on the label to promote trust. The underlying assessment criteria should be made publicly available in a transparent manner.
7. Given standards must offer a high level of trust in security. ENISA's new role must not cause existing standards to be undermined. Established high standards (e.g. ISO/IEC 15408) must continue to serve as the benchmark for a European security level.
8. The various interest groups must be closely involved with the development of the certification schemes due to their expertise and experience in these matters.

9. For assessment purposes, independent conformity assessment bodies require unrestricted access to the security-relevant data of the product or service (and their interfaces) under consideration of high data protection standards.
10. In addition to the regulation proposal, product and sector-specific requirements in respective “New Approach” regulations and directives must be reviewed and aligned with regard to information security. This requires a reassessment of risks. The aspect of the robustness of products and interoperability should be integrated into the definition of the general rules of product safety.