TÜV®

Datum
29. November 2013

Kompetenz und Unabhängigkeit bei Cybersicherheitsprüfungen in der EU stärken

Der Vd TÜV e.V. unterstützt die vorgeschlagene EU-Richtlinie über Maßnahmen, um eine hohe Netz- und Informationssicherheit in der Union zu gewährleisten.[1] Europa setzt mit der Richtlinie einen rechtlichen Rahmen für mehr Kooperation und freiwillige Initiativen in der Cybersicherheit. Zudem soll die EU-Bevölkerung stärker über die Gefahren im digitalen Raum informiert und dadurch sensibilisiert werden. Der Vd TÜV e.V. appelliert an die EU-Kommission, mit einer *Roadmap für IT-Security* langfristige Maßnahmen zur Stärkung der IT- und Cybersicherheit in Europa zu strukturieren.

Der fortschreitende Ausbau und die Nutzung moderner Informations- und Kommunikationstechnologien ist für Europa essenziell. Die zunehmende Digitalisierung von Wertschöpfungsketten unterschiedlicher Branchen, wie Verkehr, Energie, Gesundheit oder Finanzwesen, erhöht deren Wachstumspotenzial. Gleichzeitig müssen die kritischen Infrastrukturen dieser Branchen mit Blick auf den Schutz des Gemeinwesens und die Fragen der nationalen bzw. europäischen Souveränität vor Bedrohungen geschützt werden. Sowohl die Unternehmen mit kritischen Infrastukturen als auch wesentliche staatliche Stellen sollten permament die Widerstandsfähigkeit der eigenen Prozesse und der eingesetzten Informations- und Kommunikationstechnik gegen Cyberbedrohungen stärken.

Dazu gehört insbesondere die Erhöhung der eigenen Cybersicherheitskompetenz, indem geeignete Strukturen in den Unternehmen und Behörden geschaffen, die zugehörigen Mitarbeiter ausreichend geschult und mit den notwendigen Kompetenzen ausgestattet werden. Wir empfehlen hierfür die Berücksichtigung von etablierten Sicherheitsstandards, wie beispielsweise der ISO/IEC 27001 ff., die international gültigen Common Criteria und best practice Ansätze wie z.B. OWASP, die seit Jahren erfolgreich die oben genannten Punkte adressieren.

Darüber hinaus müssen speziell für industrielle IT Security Fragestellungen (Stichwort: Industry 4.0) korrespondierende weitere IT Security Standards und Normen weiterentwickelt oder zumindest harmonisiert werden. Adäquate Standards sind notwendig, um ein verlässlich hohes Sicherheitsniveau in Unternehmen und Behörden zu realisieren. Darüber hinaus sollten für Unternehmen und staatliche Organisationen, die für das Gemeinwohl kritisch erachtet werden, eine regelmäßige Überprüfung der Sicherheitsorganisation durch unabhängige, akkreditierte Prüforganisationen festgelegt werden.

Der EU-Richtlinienentwurf beschreibt die Anforderungen und Kompetenzen an die unabhängigen Stellen, die mit Sicherheitsprüfungen von Markteilnehmern und öffentlichen Verwaltungen beauftragt werden, nur vage. Diese Stellen sollten aber EU-weit einheitlich über die notwendigen Kompetenzen verfügen, die sie für die Prüfung und Zertifizierung qualifizieren. Die hoheitliche Akkreditierung[2] von unabhängigen benannten Konformitätsbewertungsstellen ist bei bereits standardisierten Zertifizierungsverfahren ein Garant für Zuverlässigkeit, Glaubwürdigkeit und Vertrauen.

[1] siehe Vorschlag der EU-Kommission KOM(2013)48 final
[2] Vgl.: Verordnung (EG) Nr. 765/2008 über die Vorschriften für die Akkreditierung und Marktüberwachung