Verfasser
Richard Goebelt

Datum
11.03.2015

VdTÜV Input to the Digital Agenda "Trust and acceptance in the digital world"

Position 1

Strengthen IT security of digital services and IT-networked production plant, and also of critical infrastructures! Promote trust in the new digital world with certificates from qualified and independent bodies!

Digital technologies have caused a disruption in industry, commerce and society. Security, along with the competitiveness and future viability of Europe, must be at the centre of this paradigm change.

The legislator has the duty to provide a well-functioning regulative framework to achieve a high level of protection for digital services, production plant and critical infrastructures.

Promotion of European IT security technologies and investment in research and development must be driven forward and underpinned financially.

Companies, organisations and institutions in the public sector must understand that data and information security is a strategic and worthwhile investment, and must design security into their activities in a systematic way.

This means developing an integrated compatible information security structure in order to strengthen trust in the digital world and raise acceptance levels. Solutions must be found which above all are aimed at minimising the time between recognition of a cyber attack and solution of the problem. Effective resistance to complex and targeted attacks cannot therefore only be centred on the IT security architecture, but must include the entire organisation, its processes and the employees involved in them. Independent certifications by qualified bodies communicate to consumers in a credible way that new and intelligent technologies are also safe, secure and trustworthy. The necessary acceptance will then follow.

Position 2

Consistently link industrial safety with digital information security in ICT applications (safety and security by design)! Encourage development of suitable safety and security architectures within organisations!

Whilst the necessity for measures to ensure safety is beyond dispute (right to life and physical integrity, industrial safety) there is still uncertainty in the field of security (protection of digital information) as to how much protection is actually needed. For example, highly-innovative products such as medical devices - which include pacemakers, dialysis machines and CT scanners - have their own IP addresses and integrated software, whose weaknesses can be used to manipulate the function of the product. The

same thing also applies to critical infrastructure, in other words highly-sensitive and essential systems such as power and water supplies.

In Europe, these are often not sufficiently protected.

It may be that information security is not systematically managed, or the technical environment may be considered separately from the IT. But as all energy and data networks are digitally controlled, and networking and data volumes are on the increase, the vulnerability of plant and equipment to cyber attack is also growing. Conventional safety must in future always be understood and managed in combination with cyber security, using a fully-integrated approach. The focus is on development of suitable safety and security architectures for conventional and digitally networked production processes. This means that all aspects of safety and security must be integrated over the entire value added chain and the complete life cycle of products, systems and software from the very beginning. The aim must be to understand both the technical and the digital world and the way they interact with each other. Then we will also create automatic alarm, analysis and evaluation tools, and so be able to identify threats, assess the risks and take effective protective measures.

Position 3

Harmonise statutory regulation and standards throughout the EU!

The greatest challenge for digitally networked production, for the transportation of the future, the smart grid and also the health sector, will be that of standardisation. The necessary integration of the new, networked systems beyond the borders of domains and hierarchies will only be possible on the basis of international, consensus-based rules and standards. They create a reliable basis for technical procurement, support communication by means of standardised terms and concepts and will ensure interoperability, suitability for practical use and market relevance.

Effective recognition and protection concepts in software applications (app security) are more important than ever for businesses and other organisations. In order to minimise the risks and eliminate weaknesses before they can be exploited by hackers, security should in future be an important performance characteristic at the product development stage. The international “Common Criteria”, which are officially recognised by the safety and security authorities in 26 industrial nations, follow precisely this approach. These CCs must, however, be adapted for industrial components and systems.

However, complex IT systems that are already in operation must also be constantly checked for their reliability and current weaknesses in order to recognise any risks at an early stage. Automated methods used up to now have often proven inadequate with regard to identification of risks, as they failed to take the context of the application into consideration. However, intelligent new processes enable automatic detection which differentiates between risks and weaknesses and therefore permits prioritisation within the protective concept - helping to save resources. This method can be used both for applications that are already operational and for software which is still under development.
In future it will be much more important for businesses and other organisations to continuously review the safety level of their IT solutions and processes and to optimise their information security management system (ISMS) by means of certification, for example based on international standard ISO/IEC 27001. One benefit of a professional information security management system is effective con-

trol of IT risks by means of systematic risk management, which means that weaknesses can be identified and potential damage and subsequent costs minimised.

Position 4

Promote cross-border and cross-sector technology partnerships throughout the EU and enable a common European market!

Safety and security in the digitally-networked world can only be guaranteed through cooperation, with nations standing shoulder to shoulder and close collaboration between industry, commerce and science. Players in these areas must remain abreast and ahead of the game: the right technical prerequisites, trained personnel, framework conditions that are suitable from the legal point of view and a high level of adaptability within the law enforcement authorities must be present throughout and at both the national and international levels.

With regard to IT security, negotiations on the Transatlantic Trade and Investment Partnership (TTIP) must aim at strengthening the security level of commercial IT products. This applies in particular to the central element of crypto-algorithms.

Skills and qualifications in the area of cyber security are not evenly distributed globally. In future it will be essential for the EU and the EU Member States to continue to develop their capabilities in the area of cyber security and to support less well protected and cyber-aware regions of the world in the fight against cyber crime.