European Office

Cybersecurity – a strategic task for Europe

VDMA statement on the 'Cybersecurity Certification Framework' (COM(2017) 477 final – 'Cybersecurity Act')

Registration number
in the register of representative bodies:
976536291-45

February 2018

1. Introduction: Cybersecurity – a strategic task for Europe

Cybersecurity is an essential cross-sectoral issue not only for the 'Internet of Things', but also for Industrie 4.0 and thus for mechanical engineering. The connectivity that goes along with the digitisation of industry is creating new opportunities for higher productivity, better resource efficiency and new areas of business. But with more players in the game, more points of contact and increasing volumes of data exchange come new risks. Digital copies of sensitive business secrets and security-related process data are embedded in networks are therefore vulnerable to disclosure.

As a technology integrator and provider of intelligent production systems, mechanical engineering plays a key role in the digitisation of industry. Networked factories produce not only physical products, but also a wealth of data. These data control and describe the production and business processes within companies and networks. At the same time, the production data are also the start of the digital life-cycle of a connected product. Industrial security is therefore a key issue also for mechanical engineering.

Production and business processes can only be successfully digitised if

- the safety of people and the environment
- the availability of equipment and services
- the protection of know-how
- the integrity of data
- the transparency of data transmission and data usage
- a secure infrastructure for data transmission
- confidentiality
- compliance with existing legal and contractual obligations
- and transparency and standardisation of interfaces

is assured. Cybersecurity contributes significantly **–** albeit to a varying degree **–** to achieving these objectives, making it a strategic task for companies.

Cybersecurity is not an end in itself: it protects systems and infrastructures from attack, thereby contributing to protection goals such as safety (protecting people and environment), data privacy and availability of public and private services. This helps to reduce the risks that can arise when production and business processes are interlinked.

Companies are already investing in security as part of their business interests, and security aspects are increasingly an element of the quality requirements within value chains. It can therefore be assumed that in some cases security goals are already achieved by means of established market mechanisms and arrangements under private law. Nevertheless, there are areas where European lawmakers are required to take steps to ensure the achievement of higher-level social protection goals. But it is vital that legislators does not consider security as an isolated sub-domain or as belonging solely to the IT sector; instead, it must be regarded as part of the European single market and of global value chains.

2. The ball is rolling, but a second strike is needed

Europe is called upon to create a single market infrastructure for cybersecurity that is globally compatible and builds trust within digitised value chains, while not unduly restricting innovation and competitiveness.

However, the certification framework set out in Title III of the 'Cybersecurity Act' ('Cybersecurity Certification Framework') is only suitable for a portion of the products, systems and processes under threat from cyber risks. The Commission's proposal is more in line with the characteristics of a voluntary quality label for meeting cyber requirements. The mechanical engineering sector sees rather the need for a horizontal regulation which would cover the marketing of ICT products and which would make regulation of Cybersecurity part of the EU single market. Particularly for industrial business-to-business networks such as mechanical engineering, the proposed framework fits only in a handful of cases – partly because the certification instrument preferred by the proposal can be an effective solution only for a small number of applications.

The proposal unfortunately disregards the use of the tried and tested single market infrastructure of the 'New Legislative Framework' ('NLF'). It lacks essential elements such as the proven interplay between the specification of basic requirements by lawmakers and the more detailed articulation of those specifications by standards organisations, the linkage to market surveillance and the rules for conformity assessment. From the point of view of the VDMA, the 'Cybersecurity Act' can therefore be not the ultimate step and is not suitable for broad deployment in heterogeneous, internationally dynamic value networks as with Industrie 4.0.

However, the Commission's proposal does offer the chance to reduce emerging and existing fragmentation as a result of national certification systems in the EU. It is positive that this approach utilises the knowledge existing within Member States and provides the opportunity to take action at those points where the Member States and the sectors involved consider it necessary. On the other side, there is a need for improvement with regard to the involvement of the business community and the international compatibility of the arrangements. But if these points are clarified and improved in the further legislative process, the certification framework can be at least an acceptable first step.

From the perspective of the VDMA, however, a distinction needs to be made between two approaches:

- **The Commission proposal on the Cybersecurity Act needs to be improved in order to ensure global compatibility, guarantee transparency and clarify governance. This can best be achieved through a single market provision based on the principles of the New Legislative Framework ('NLF'), to be applied by the manufacturer to IT products. Such a provision would be a stand-alone European legislative solution for cybersecurity in the form of a horizontal cybersecurity rule ('phenomenon directive').**
- **However, if no single market rule for the cybersecurity of IT products is envisaged, voluntary 'Certification Schemes' drawn up on the basis of the certification framework are a potential compromise. In such case, however, the manufacturer must be able to decide whether or not the IT products to be marketed should bear the 'quality label' so regulated.**

3. Key messages and recommendations on the 'Cybersecurity Act'

As part of a comprehensive EU Commission package on cybersecurity (JOIN(2017) 450 final), the certification framework proposed in the 'Cybersecurity Act' aims to avoid fragmentation through regulations at Member State level. This objective is fundamentally correct and the VDMA supports it, as it does the EU Commission's entire strategic initiative on cybersecurity. However, the VDMA considers it necessary to improve and clarify the following points:

Certification – especially that of products – is suitable only in a limited capacity to meet the challenge of 'security'. Not only certificates, but all available instruments for conformity assessment must be utilised – such as the manufacturer's self-declaration. The choice of instruments must be appropriate and must avoid excessive bureaucracy, costs and obstacles to innovation.

The proposal on the 'Cybersecurity Act' only provides for third-party certification. Due to the constantly changing threat situation ('moving target') and the rapid pace of innovation in the sectors concerned, such as IT and IoT, and in the context of digitisation in general, however, it is fundamentally debatable whether this focus on certification is appropriate and effective.

Certification processes are expensive and time-consuming for manufacturers. They prolong the time to product launch, generate high costs, and inhibit innovation. In addition, especially in mechanical engineering, customer-specific solutions are frequently needed. If these required a certificate, this would entail disproportionately high costs and effort for each individual case. New technologies often also require new testing rules, which might not be available without a considerable delay. This creates an additional obstacle to the introduction of new technology, including for existing ICT products. There is a risk that certification processes could even hamper the updates and innovations that are so vital for security. In B2B sectors such as mechanical engineering, labels and certificates only rarely offer any benefit, and are largely seen by companies in a negative light, as a recently published study by the VDMA's IMPULS Foundation confirms[1].

Instead of favouring certification as a blanket measure, the successful element of conformity assessment must be utilised. The existing conformity assessment modules (768/2008/EC) offer a range of options that would greatly facilitate the application of appropriate assessment procedures. For instance, the use of the modules relating to internal production control and quality assurance appears fit for the purpose (Module A for internal production control and Module H for evaluation of the manufacturer's capabilities).

Improve governance: certification must be driven by economic operators, not by public authorities. Implementing acts may only define basic requirements; the formulation of the concrete protection goals must take place within the framework of European and international standardisation.

The proposed certification framework provides that the certificate systems will be devised almost exclusively by public authorities at national and European level. It also provides for the awarding of certificates by public authorities.. However, government certification systems

[1] https://www.vdma.org/documents/105628/21813053/IMPULS-Studie_Labels-deutsch_1510043826190.pdf/01680e2d-458c-43f0-9ce1-d6d472e5b597

and the award of certificates by public authorities are incompatible with requirements on international markets. For effective and internationally compatible systems, it is essential that the certification be primarily driven by economic operators. The proposal needs to be significantly improved on this point.

It is especially important that the definition of the basic requirements and the formulation of concrete measures be assigned to the appropriate level. Regulatory approaches that merely formulate basic legal requirements and otherwise refer to the European standardisation system would be expedient and ease the burden on governments. Implementing acts and comitology do provide Member States with a right of co-determination, and thus the opportunity to use existing know-how and progress at national level. But they cannot reflect the demands of economic operators and international markets.

The VDMA therefore proposes that the envisaged implementing acts only define basic security requirements for each specific application or product category of a 'scheme'. Article 45 should be revised accordingly. The list of cybersecurity requirements in the present form is incomplete and is not flexible enough to respond to new challenges (the list is obviously a sub-set of the requirements from ISO/IEC 27001).

After a standardisation mandate has been issued, the formulation of concrete protection measures and of the state of the art must then be based on European standardisation, preferably in cooperation with international standardisation bodies. Through the use of such standards, effective and innovative solutions for achieving the security protection goals will be developed, and it will be avoided having the European economy cut off from international developments.

Review the description of the security levels in Art. 46

Article 46 proposes three different 'assurance levels'. This needs to be fundamentally re-examined and revised, as any such different levels in the market would tend to muddy the waters rather than provide clarity: a high 'assurance level' may cause people to conclude that that the product guarantees absolute security, which is not the case. A lower level, on the other hand, would always be regarded as 'inferior'. For instance, it is questionable whether a certificate for an 'Assurance Level basic' with the description 'limited degree of confidence' is likely to increase trust.

Instead, any future conformity assessment procedure should be based on clear legislative requirements. The VDMA does not consider the introduction of different levels in this form necessary.

Apply principles of good regulation policy, embed 'checks and balances', ensure transparency

Although voluntary, the systems envisaged should engender trust and be broadly acceptable. For this to happen, it is essential that proportionality be maintained and that the necessity or suitability of a certification system be carefully assessed before any introduction. It is therefore crucial that the process be transparent and that it be provided with an effective system of checks and balances. The following elements must therefore be added to Art. 44:

- The careful examination of the need for and suitability of a certificate system must be embedded in the process and must follow an appropriate test procedure. The above-mentioned study on the use of labels carried out by the VDMA's IMPULS Foundation describes such a scheme.

- The regular publication of a work plan to inform the public and all interested parties, in a comprehensible and transparent manner, in which areas certificates are to be developed next.
- The embedding of a catalogue of quality criteria for good legislation in Art. 47 (2): certain basic principles must be observed when developing a new certificate, to avoid any undesirable effects in terms of competition, existing legislation or end users. These basic principles include, for example, technological neutrality, proportionality, protecting the competitiveness of the regulated industry, and avoiding double regulation.

4. Summary and conclusion:

From the perspective of the VDMA, the proposed certification framework is broadly unsuitable to bring about an effective increase in cybersecurity in industrial value chains (including mechanical engineering), as it aims at certification that is effective only within certain limits. It does not seek to establish a comprehensive horizontal single market solution.

The ideal would be, in the view of the VDMA, a stand-alone single market rule for cybersecurity according to the principles of the New Legislative Framework ('NLF'). As an innovation-friendly and flexible legal regime, such a cybersecurity provision not only offers economic operators the necessary flexibility and freedom to innovate, it also relieves the burden on Member States, the Commission and ENISA by removing the need for permanent activities associated with the preparation of the required 'certification schemes'.

However, the proposal on the 'Cybersecurity Act can be a first acceptable step if it is improved in the further legislative process and, in particular, if it corrects the wholly government-driven procedures towards the certification systems. Certification – if deemed necessary – must be driven by the economic operators and concrete protection goals and measures must be worked out within the framework of standardisation.

Contact:

Naemi Denz
VDMA Technology, Environment and Sustainability
+49 69 6603 1226

Kai Peters
VDMA European Office
+322 7068219

Steffen Zimmermann
VDMA Competence Center Industrial Security
+49 69 6603-1978