FIEEC
FEDERATION DES INDUSTRIES ELECTRIQUES, ELECTRONIQUES ET DE COMMUNICATION

ZVEI
Die Elektroindustrie

Position Paper

Joint FIEEC-ZVEI Position on Cybersecurity

October 2017

Preface

The digital transformation of the European economy and society opens up great possibilities for competitiveness, growth and jobs. Our European industries are in the process of becoming digitised at high speed: the digitalisation of products, processes, and systems as well as the creation of innovative and new business models are developing. Similarly, digital platforms, services and sales opportunities change the relationship between customers and company relations. The Internet of Things (IoT) transforms traditional role models especially in the manufacturing sector. From industrial suppliers, manufacturers become integrators and service providers.

The European Union's Digital Single Market strategy and Digitising European Industry Initiative successfully support this digital take-up. In this context, our industries highly depend on trust and confidence within a common Digital Single Market. For this reason, our industries have identified cybersecurity as a pre-condition and fundamental need to make digitisation happen and to build trust for both companies and consumers. Furthermore we consider cybersecurity a strategic issue for Europe to gain competitiveness in a global market economy.

Following the FIEEC-ZVEI Digital Conference of July 2016 (Joint Declaration, Joint Position Paper), both associations have decided to cooperate on a joint cybersecurity position. This position is the result of a common understanding and regular exchanges between FIEEC-ZVEI cybersecurity experts. FIEEC and ZVEI represent 4 600 companies including suppliers and users of cybersecurity solutions and products, 1,249 million employees and a turnover of 278,5 billion euros.

The ambitious European Cybersecurity Package, which has been proposed by the European Commission on 13th of September, is an important step in the right direction. FIEEC and ZVEI have acknowledged this initiative as a relevant tool in order to further strengthen the EU's cyber resilience and step up capacities across the society and economy of member states,. Nevertheless, this package cannot be seen as a monolithic block of objectives and operations to tackle challenges in cyberspace. With respect to the debate on cybersecurity, FIEEC and ZVEI are taking stock of existing and new European initiatives and propose their guidelines to policy makers and involved stakeholders based on the following joint positions and principles:

Firstly, this French-German position highlights the importance of cybersecurity within the Digital Single Market. Secondly, it provides recommendations from our members to build an innovation-friendly, robust and improved European Cybersecurity Union.

The French and German electrical and electronic industry associations call for a flexible but resilient market-driven European framework for cybersecurity. Such a framework should take industrial needs and innovation into account and should offer adequate and applicable security solutions to make products, systems and manufacturing systems safe for the digital age.

Such a framework should be based on harmonised international or at least European security standards, harmonised certification and qualification schemes where applicable, with the highest possible level of transparency, coherence and information for end-users and customers. Furthermore, this framework should apply to the specific dimensions of cybersecurity as a moving target.

European policy makers should concentrate on a cohesive and coordinated approach to foster European cybersecurity resilience in a sustainable and fit-for-purpose manner. This includes a close partnership and a regular, effective cooperation with industrial initiatives, stakeholder platforms and associations like the Alliance of the Internet of Things Innovation (AIOTI) or the European Cybersecurity Organisation (ECSO).

This common understanding of the French and German electrical and electronic industries calls for confined, targeted and differentiated solutions with respect to the use of smart devices and the internet of things. Any regulation on IoT should be precisely justified and defined in terms of need, scope, impact and effectiveness. Especially when considering the fact that Business-to-Consumer and Business-to-Business markets cannot be easily separated from each other anymore.

I European Framework / Toolbox for Trust and Cybersecurity

In this context, our Associations are especially aware of the presentation by the European Commission of a Joint Communication entitled "Resilience, Deterrence, Defence: Building strong cybersecurity for the EU" and a proposal for a regulation on ENISA and on ICT cybersecurity certification, in order to improve cybersecurity in Europe.

FIEEC and ZVEI welcome the fact that the European cybersecurity certification schemes would be defined at a European level in order to minimise the fragmentation between member states and the fact that these schemes remain voluntary.

Concerning the three proposed security levels (basic, substantial, high), we recommend defining the requirements on sectoral approaches. When the highest levels of security are required for security products, the new certification scheme shall not degrade the security assurance provided by currently available certification schemes.

From this perspective, FIEEC and ZVEI are calling for a European Cybersecurity Framework, which creates trust and confidence based on the following benchmarks:

- A risk-based approach is essential for any B2C, B2B or critical infrastructure (CRITIS) regulatory framework. Governments, CRITIS, business or consumer markets, either IOTs or industrial IOTs (IIOT), face different risk exposure and vulnerabilities, thus they need different requirements and solutions. This is why different security levels and risk assessments should be defined according to the need of users for trust and confidence.
- FIEEC and ZVEI support a multilevel toolbox that consists of four key elements:

  1) Security standards for products and processes for IoT and IIOT devices.

  2) An EU-wide self-declaration scheme for cybersecurity for B2C and B2B markets that reflects the level of security measures and not the level of security assurance, to be integrated as a possible option alongside certification schemes.

  3) Independent and third-party assessment depending on market needs and based on a risk-based approach, especially when addressing the high-level security requirements (typically EAL4+ and above).

  4) Security entry level for products should in principle be achievable without third-party involvement based on harmonised standards.

Since cybersecurity becomes more and more relevant for the functional level and safety of smart devices in operating systems, it strongly affects EU rules for product placing on the market. Given the importance of the single market, FIEEC and ZVEI recommend the following principles as a foundation for a European toolbox:

1) **Scalability:**
   The toolbox should work regardless of whether the product is sold only once or a million times.

2) **Flexibility:**
   The toolbox should work for a broad range of products (consumer to industry) – ideally for upcoming products too.

3) **Uniformity and Comparability:**
   The toolbox should provide consistent and comparable information for consumers and users across the EU.

4) **Adequate for shorter (digital) life cycles:**
   The toolbox works even in time- and cost-sensitive markets.

5) **Effectiveness:**
   The toolbox highlights cybersecurity as a product quality feature and provides a starting point for secure integration and operation.

6) **European Recognition of Certification Laboratories:**
   The laboratories that will test any critical product should be recognised at a European level after an assessment by a peer external party (accredited body).

For all activities by the Commission, member states, or industries, standardisation is key. International or European security standards define requirements, hence the need for state of the art security. In addition, they support open markets and decrease market fragmentation as well as transaction costs. Any framework, toolbox, or policy option should, therefore, take into account the requirements and information security management for IT (ISO 2700x), industrial automation and control systems for OT (IEC 62443), and industry sector-specific standards.

FIEEC and ZVEI highlight that it is of utmost importance (a) to fully involve industry in the governance process defining standards, and (b) for scope, content and requirements to be elaborated and applied under a European certification scheme.

II A Need for Coordination at a European Level

We appreciate the European Commission's ongoing initiatives on cybersecurity. FIEEC and ZVEI are aware of an increasing number of initiatives, platforms, and actors that are involved with cybersecurity and ICT certification:

- Actors: portfolio of commissioners (Ansip, Gabriel, Bienkowska, Sir King), DG CNECT, DG GROW, DG HOME, DG ENERGY, DG RESEARCH, ENISA, JRC,
- Platforms: CSCG, AIOTI, Industry Leadership Group (ESIL), SOGIS, ESO/ ECSO, MSP, Eureka,
- Standardisation Bodies: IEC, ISO, CEN/CENELEC, ETSI,
- Regulation: NIS, GDPR, eIDAS.

Hence, the existence of multiple interdependencies and overlapping proposals can lead to potential confusion and should definitely be clarified. FIEEC and ZVEI both identify a need for:

- Taking stock of the global nature of digitisation, in particular for standardisation. Any standardisation initiative at a European level should first reflect the global work by Standards Development Organisations. Generally speaking, we need to promote the concept of "global chain of trust" e.g. within standardisation bodies (ISO, IEC, ITU), international governance regimes (OECD, G20,) or trade negotiations and agreements.
- A coordinated action on cybersecurity standardisation, within the framework of the Technical Committee Cybersecurity and Data Protection of CEN-CENELEC TC 13.
- Any European ICT security product regulation should be based on the New Legislative Framework (NLF, 2008). According to the requirements for accreditation and market surveillance, this framework sets out the basis for mandatory requirements and practicable conformity assessment mechanism for ICT products and services. European Standardisation Bodies should develop industry-driven standards complying with the conformity assessment of security requirements with respect to the NLF.
- A tailor-made approach; hence not applying the same rules, nor the same approach, to every economic sector, especially in a context of B2B relations.
- A stronger cooperation and effective coordination within and across European Institutions (DG CONNECT, DG GROW, DG HOME, ENISA, etc.…) on cybersecurity issues.
- The harmonisation of existing and emerging national certification schemes (such as the French CSPN certification scheme etc.) that apply at a European level and to the Single Market. This is absolutely necessary. It would avoid further national fragmentation and should be applicable to existing schemes at a global level for operational technologies (and not only for information technologies…).
- A coordinated action on cloud assessment/certification at European level, compliant/linked with the ANSSI & BSI initiative & compliant with cloud & security standards (CSA STAR, 27001,…). It is also necessary to recognise the work of ENCRIP, to avoid market fragmentation through mutual recognition, which can (only) be a first step.
- Better consistency and explicit differentiation between European privacy and security regulations (NIS, eIDAS, GDPR, e-Privacy Regulation). Legal certainty and clear distinction in regulation are essential for market operators and sound digital innovation.
- Promoting the concept of security-by-design as the result of secure product development, product quality assessment and documentation alongside the lifecycle of products and processes, which need be taken into account.
- Creating soft incentives, which encompass the security of hardware, software, and processes within industrial production and cross-sectorial value chains, in order to promote the concept of industrial security.
- Promoting the role of SMEs to widely adopt cybersecurity solutions as part of major European industrial processes and production lines.
- Promoting the need for more digital self-responsibility and liability in consumer markets.
- Promoting the important role of awareness and information sharing tools among companies and governments across the EU in order to respond quickly and effectively to cyberattacks.

Joint FIEEC-ZVEI Position on Cybersecurity

Publisher:
ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e.V.
German Electrical and Electronic Manufacturers' Association
Lyoner Straße 9
60528 Frankfurt am Main, Germany
Contact: Cornelius Eich, E-mail: eich@zvei.org
Lukas Linke, E-mail: linke@zvei.org

www.zvei.org

October 2017

FIEEC Féderation des Industries Electriques Electroniques et de Communication
17 rue de l'Amiral Hamelin
75783 Paris Cedex 16, France
Contact: Guillaume Adam, E-mail: gadam@fieec.fr
Yoann Kassianides, E-mail: ykassianides@fieec.fr