Cybersecurity and business resilience for SMEs

Dr. George Sharkov

Director, European Software Institute – CEE (Bulgaria)

gesha@esicenter.bg

Expert @ETSI TC CYBER

Nominated by PIN-SME through SBS (Small Business Standards)

ETSI TC CYBER – established in 2014, 2 meetings
Next meeting #4: 25-26 June 2015 (Sophia Antipolis, ETSI)

Scope:

- Cyber Security
- Security of infrastructures, devices, services and protocols
- Security advice, guidance and operational security requirements to users, manufacturers and network and infrastructure operators
- Security tools and techniques to ensure security
- Creation of security specifications and alignment with work done in other TCs

ETSI CYBER: responsibilities

- To act as the ETSI centre of expertise in the area of Cyber Security
- Advise other ETSI TCs and ISGs with the development of Cyber Security requirements
- To **develop and maintain the Standards, Specifications** and other deliverables to support the development and implementation of **Cyber Security standardization** within ETSI
- **To collect and specify Cyber Security requirements from relevant stakeholders**
- To identify gaps where existing standards do not fulfil the requirements and provide specifications and standards to fill these gaps, without duplication of work in other ETSI committees and partnership projects
- To ensure that appropriate Standards are developed within ETSI in order to meet these requirements
- To perform identified work as sub-contracted from ETSI Projects and ETSI Partnership Projects
- **To coordinate work in ETSI with external groups such as Cyber Security Coordination group in CEN CENELEC and ENISA**
- **To answer to policy requests related to Cyber Security, and security in broad sense in the ICT sector.**

GS: Focus on SMEs

Areas of interest, weak and sensitive for SMEs, that are considered to be discussed for the next TC meetings:

- Privacy and regulations – also related to security by design (for IT/software companies), and at the user level
- Basic security requirements – in relation to ENISA recommendations, and connected with the European Cybersecurity Strategy (of 2013) and the expected EU Directive on NIS (which also includes IT/Cyber risk management, specific section on SMEs)
- I plan to raise the issue of standardization of internet security for smart devices (IoT, Internet of things) – that is in connect ion with other TCs of ETSI, also CEN/CENELEC – applicability, and affordability for SMEs, and also requirement and incentives

SMEs not in the Cybersecurity focus (yet)

Aspects not considered currently by standards and policies in the Cybersecurity area (EU, and globally – ITU, ENISA, NATO, national, etc.):

1. Cybersecurity vulnerabilities and threats for everyday users in small business – minimal awareness requirements (skills and competences), trainings and awareness guidelines (education & training), job profiles (employment)

2. Minimal compliances and requirements for small IT/software related businesses ("garage" companies, freelancers, startups, etc.)

3. Methodology and standard for Shared Risk assessment and mitigation over a "value chain":

- in supply chains as providers/suppliers
- "in the middle" – they also have suppliers, outsourced activities
- no "digital dependency" assessment of daily services and operations, no minimal security requirements (compliances), no qualification requirements, and no design requirements

Advocate for EC directives and regulations, and for standards and recommendations form ETSI TCs, CEN/CENELEC

Other engagements

- EC – ENISA, NISP (Network and Information Security Platform) – WG1 (Cybersecurity and risk assessment models); WG2 (Information sharing) – related to European Cybersecurity Strategy (2013)& Directive on NIS (expected end of 2015)
- CEN - WS on ICT skills
- CEN – PC 428 “e-CF and IT professionalism”
- ESCO – ICT SRG (Bulgaria), ICT job profiles
- NATO- NCIA/DNBL