Press Release

2016/01/19 | EPR03/2015 | www.enisa.europa.eu

ENISA’s ten messages to industry at Berlin IT security forum

“Technological developments such as Internet of Things, Big Data and Smart Devices are becoming the driving force behind many IT companies. Issues related to security and privacy, if not addressed appropriately, may have an impact on the growth of the IT market” said ENISA’s Executive Director, Udo Helmbrecht, discussing on the state-of-play of IT security at a panel with German Federal Minister of Economic Affairs and Energy, Sigmar Gabriel, and industry representatives including Rüdiger Stroh (NXP Semiconductors), Vera Schneevoigt (Fujitsu) and Thorsten Dirks (BITKOM).

At the forum, organised by the German Ministry of Economic Affairs and Energy, on January 19th, Helmbrecht, noted the need for cooperation among all stakeholders is fundamental in order to build on concrete approaches which can fit and stimulate the sector. “ENISA promotes the development of approaches to security that are not hampered by national restrictions or particular communities so that solutions are cost-efficient and interoperable across the EU”.

The recent agreements on the NIS directive and the European General data Protection Regulation (GDPR) impose new network and information security requirements on operators and digital service providers, and require incident and privacy breach reporting, subjecting companies to change their operating model and comply with more stringent specifications. ENISA focuses on establishing a high level of cybersecurity across all industry segments, and ensure cybersecurity acts as an enabler for industry to capitalise on as a differentiator factor for products and services. ENISA recommends to:

- **Consider new business models that capitalise on security as a differentiator of products and services.**
- **Establish sectorial requirements for information security in order to move the cybersecurity market.** By creating common requirements representative of entire industry sectors, industry can influence supply and move the market to reflect their needs.
- **Reduce Operational Expenditure by Improving Risk Management**
- **Secure the whole lifecycle of products by using security and privacy by design.** Equally, it is important to validate the security of the supply chain and to ensure the secure integration of all components together.
- **Improve cooperation within and across industry segments and national borders to improve threat intelligence and promote the application of good practices.** Opportunities exist for closer collaboration with EU policy makers, to improve the competitiveness of EU industry in the global market. Notable examples include the DSM, GDPR initiatives. Improving threat intelligence and spreading best practice, benefits all industry players and reduces costs.

ENISA’s recommendations and the **full paper** are available online**.**

For interviews and media enquiries please contact **press@enisa.europa.eu** , **Tel.** +30 2814 409576