ENISA maps the Threat Landscape for Internet Infrastructure in 2014 and provides a Good Practice Guide for enhanced security

ENISA's Threat Landscape and Good Practice Guide for Internet Infrastructure published today, maps the assets composing an Internet infrastructure and the applicable threats, giving an overview of emerging trends, and providing adapted security measures. The report is targeted primarily at Internet infrastructure owners, as well as Internet organizations, security experts, developers of security guides, and policy makers.

The report details the assets composing an Internet infrastructure and classifies the threats applicable, highlighting "important specific threats" that disrupt connectivity. These include routing threats, DNS threats, and (Distributed) Denial of Service. Each threat is linked with a list of assets exposed. Overall, there is an increase in the occurrence of these threats.

The report takes stock of publicly available security measures to protect Internet infrastructure assets and will enable asset owners to carefully analyse their Internet infrastructure through risk assessment and evaluation of exposure to specific threats. It details a list of good practices to make an Internet infrastructure more secure.

Furthermore, a gap analysis outlines existing shortcomings of current good practices. From the analysis, the gaps are linked to the application of skill sets in all important specific threats analysed, as well as to system configuration and essential addressing protocols for (Distributed) Denial of Service.

Five technical recommendations and four organisational recommendations respectively, are proposed for an enhanced level of security through the development and application of good practices, and the importance of collaboration in the community.

Udo Helmbrecht , ENISA's Executive Director, commented on the project: *"Threats analysed in the current study indicate they are globally on the rise. It is important to apply good practices and promote the exchange of information, in order to mitigate threats and secure Internet infrastructure. ENISA's Guide gives an up to date overview of emerging threats and lays the foundations for the community towards a more secure Internet infrastructure through proper risk assessment, training and evaluation".*

The publication is part of the ENISA Threat Landscape 2014, an activity towards achieving the objectives formulated in the Cyber Security Strategy for the EU, which stresses the importance of threat analysis and emerging trends in cyber security.

For full report: Threat Landscape and Good Practice Guide for Internet Infrastructure

For interviews: Dr. Louis Marinos, Network and Information Security - Research and Analysis Expert, ENISA, **Email:** louis.marinos@enisa.europa.eu, **Phone:** (+30) 2814409682