Emergency Response to Security Breaches

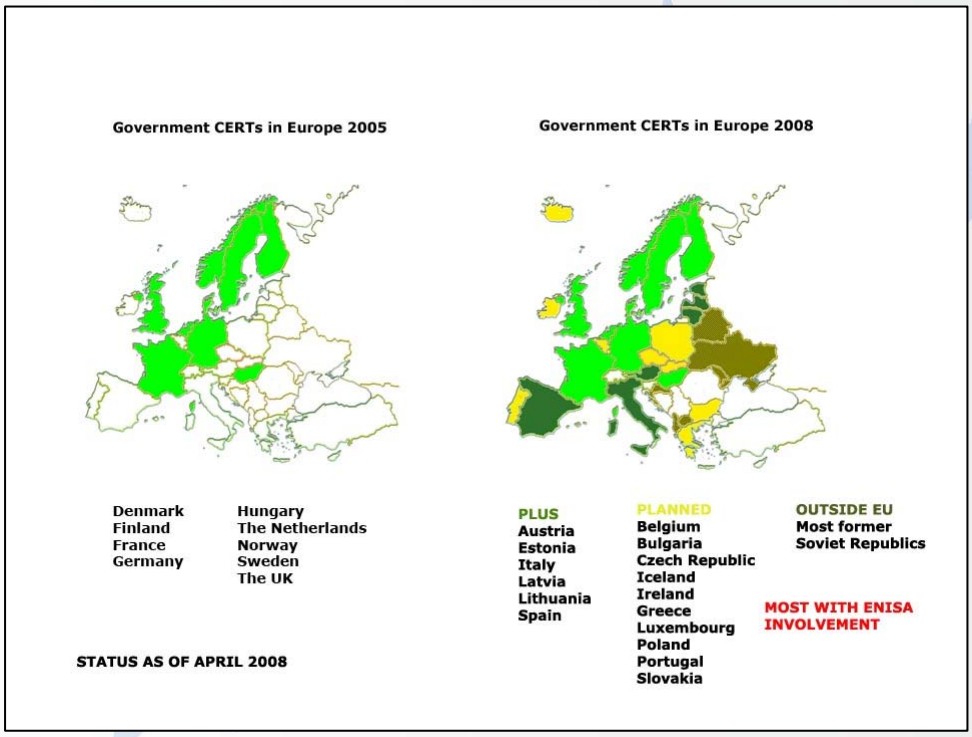


Figure 1: CERT network in Europe as of April 2008

What is a CERT?

CERT stands for Computer Emergency Response Team. A more recent term is Computer Security and Incident Response Team (CSIRT) The name explains what makes these entities so special: like a fire brigade, they are the only ones that can react in case of security incidents.

Besides reactive services (incident response) they usually also provide a comprehensive portfolio of other security services for their customers such as alerts and warnings, advisories and security training.

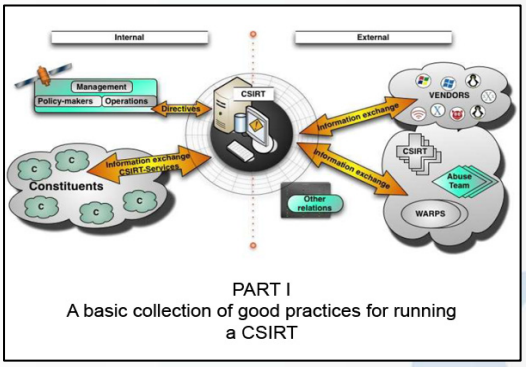
Over the years, CERTs/CSIRTs have evolved into premium providers of security services.

Why is ENISA involved?

Cyber attacks in Estonia and towards governments in Germany, Sweden, France and other countries have increased interest in CERTs/CSIRTs. Some time ago, teams across Europe identified co-operation as a necessity for successful incident response. This is because attacks from the Internet do not stop at traditional borders, but concern all aspects of the Information Society. Since the early 1990's, collaboration has occurred in communities such as Terenas Task Force CSIRT (TF-CSIRT) and the European Government CERT Group. These growing communities are essential as rich sources of information, tools and activities for network and information security.

ENISA's role is not operational, but rather it acts as a facilitator and information broker for CERTs/CSIRTs. As an EU Expert body, it must stay in touch with all the CERT/CSIRT communities – in Europe and beyond.

PO Box 1309, 71001 Heraklion, Greece, Tel: +30 2810 391 280, Fax: +30 2810 391 410
www.enisa.europa.eu



PART I
A basic collection of good practices for running a CSIRT

So there should be a CERT for every internet user?

In an ideal world, yes! But many factors – not least financial – prevent the full coverage of all users with every available security service. But there are other entities that offer necessary services which are not 'fully grown' CERTs. The *Abuse Teams* of the big Internet Service Providers (ISPs) for example contribute to spam and abuse handling. Hard- and software vendors make available security information about their products. Finally, community-driven Warning and Alerting Points (WARPs) support their members by sharing security relevant information. ENISA has to keep abreast of these activities to support them in their coverage of users and provide advice to the Member States on improving provision of security services for EU citizens.

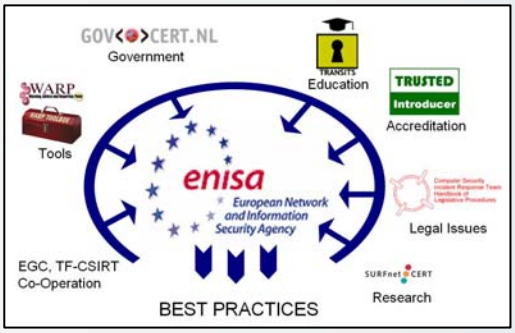
So what is ENISA's role?

ENISA has initiated contacts with relevant global players in the CERT field. The Agency met representatives from FIRST, TF-CSIRT, the American CERT/CC, Asian-Pacific-CERT and the National Computer Network Emergency Response Technical Team/Coordination Center of China. ENISA has visited the WARP communities in the UK and co-organized training courses in Europe with the TRANSITS team. The Agency has also lent its expertise to various events and conferences. Finally, ENISA collects and disseminates best practices, e.g., *Step-by-Step Approach on How to Establish a CSIRT* and *Good Practices for Running a CSIRT*. In 2008 ENISA will publish a handbook for CERT exercises which will be piloted in 2009.

And in the future?

ENISA will continue to support the establishment of entities like CSIRTs and WARPs. Moreover, the Agency will examine measures on how these entities can maintain and improve the quality of their security services. ENISA will analyse features like advanced training, possible scenarios of certification or incident response exercises and compile a best practices document.

The Agency will also enhance its ability to advise Member States on how to improve IT security in their countries based on an assessment of user security service needs. ENISA will continue to produce good practice guides in the field of CERTs in the future and test them in pilot conditions.



I want to know more…

Please visit our website regularly (http://www.enisa.europa.eu), or email us at info@enisa.europa.eu) and you will soon be set in contact with our CERT Experts.

PO Box 1309, 71001 Heraklion, Greece, Tel: +30 2810 391 280, Fax: +30 2810 391 410
www.enisa.europa.eu