enisa
European Network and Information Security Agency

Emergency Response to Security Breaches

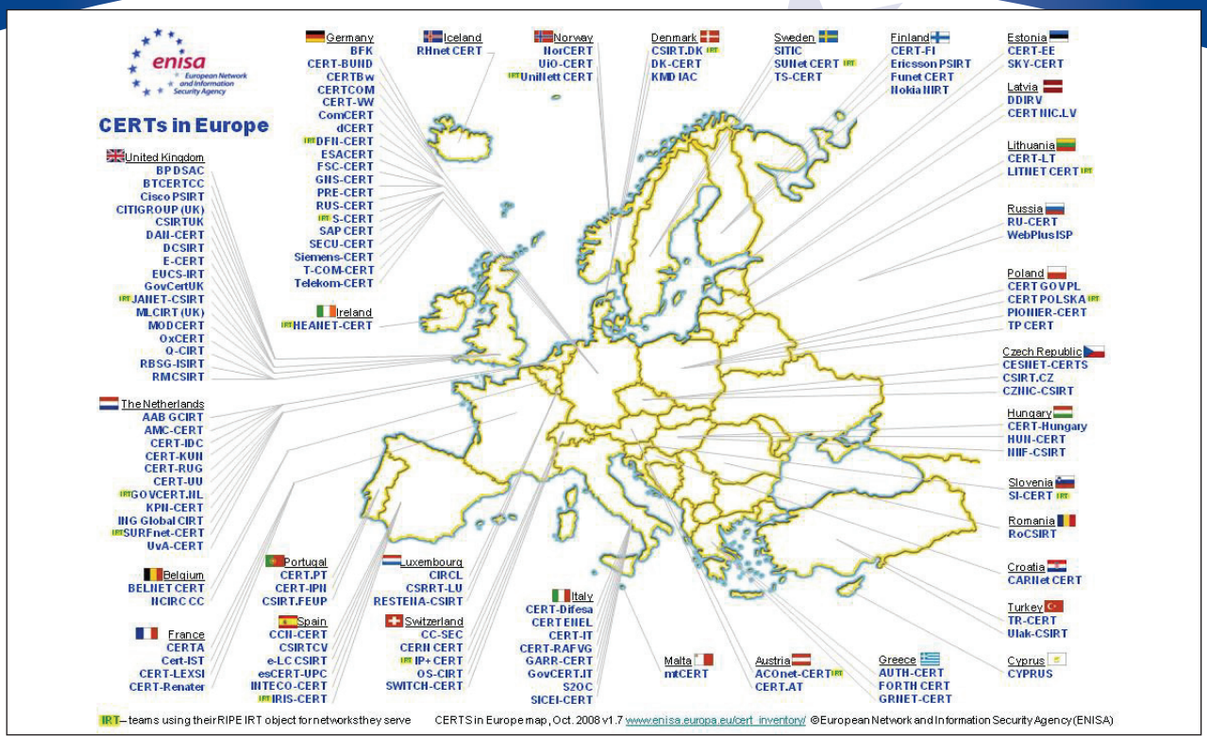


Figure 1: CERT network in Europe as of October 2008

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 which can react when security incidents occur.

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 on the Internet do not stop at traditional borders, but concern all aspects of the Information Society.

Since the early 1990s, collaboration has been taking place through communities such as the Terena's Task Force CSIRT (TF-CSIRT) and the European Government CERT Group. These growing communities are essential because they are 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

enisa
European Network and Information Security Agency

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. There are however other entities which are not 'fully grown' CERTs but which do offer the necessary services.

The *abuse teams* of the big Internet service providers (ISPs), for example, contribute to spam and abuse handling. Hardware and software vendors make security information about their products available. Finally, community-driven Warning and Alerting Points (WARPs) support their members by sharing security-relevant information.

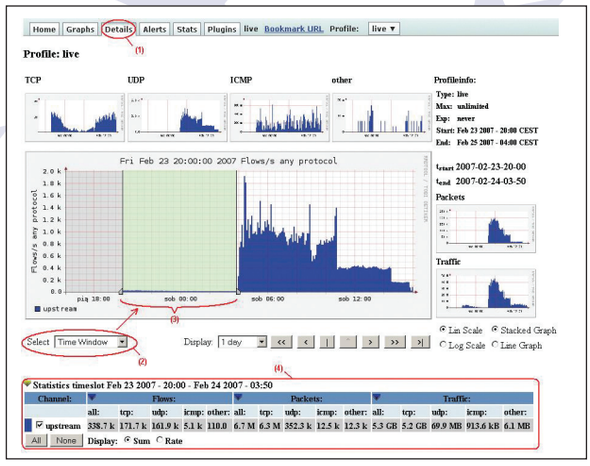
ENISA has to keep abreast of the activities of these entities to support them in their coverage of users and to provide advice to Member States on improving the provision of security services for EU citizens.

So what is ENISA's role?

ENISA has initiated contacts with relevant global players in the CERT field. The Agency has 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 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., in its publications *Step-by-Step Approach on How to Establish a CSIRT* and *Good Practices for Running a CSIRT*. ENISA has published a handbook of CERT exercises which is being piloted in 2009.



Network monitoring - CERTs guarding the networks!

And in the future?

ENISA will continue to support the establishment of entities such as 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 such as advanced training, possible scenarios for certification or incident-response exercises, and will 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 and test them under 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 put 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