Resilient Networks
Information Sharing Exchanges

Is there a need for an NSIE?

Information sharing is among the most common forms of cooperation between stakeholders.

It is considered as a means to:

✓ Better understand a changing environment
✓ Learn in a holistic manner about intrusions, vulnerabilities and threats
✓ Develop jointly recommendations for reducing network security vulnerabilities, threats, and attacks
✓ Develop jointly methods to continuously assess existing measures

Provide unique insights and strategic views to policy makers and strategists.

Information Sharing Exchanges

Information sharing exchanges are necessary to better understand the constantly changing environment of communication networks.

Member States are strongly interested in better understanding and deploying the concept of a ‘Network Security Information Exchange’ (NSIE).

They requested ENISA to develop a good practice guide. The guide will assist them and other relevant stakeholders in setting up and running national NSIEs.

Such a guide will hopefully pave the way for an accelerated deployment of national NSIEs and consequently of pan European one.

Characteristics of an NSIE

✓ The most effective size of a sharing group is between 20 and 30
✓ Regular, face-face meetings to establish and further enhance trust
✓ government role is instrumental in setting up and running an NSIE together with industry

✓ An NSIE addresses strategic issues (e.g. major/critical disruptions) rather than operational ones
✓ Participation is free of charge
✓ New members require the unanimous agreement of existing members
✓ most existing NSIE’s are jointly chaired by a representative from the government and a representative from industry
✓ An NSIE should provide with incentives their members to participate
✓ An NSIE should respect members commercial sensitivities related to the disclosure of information to competitors and/or regulators
✓ Emphasis is on information exchange, not on information transfer
✓ High level security experts usually participate in NSIES

What is shared?

✓ Experience and information on threats, risks, impact, vulnerabilities, incidents, counter measures
✓ Advisory support and warnings in implementing joint, sector wide, protective good practice measures
✓ Experience and information on:
  ✓ contingency planning
  ✓ crisis management
  ✓ analysis & mitigation of threats, risks, incidents, dependencies
✓ Information on emerging trends and changing environments
✓ Information on exercises, on methodologies and scenarios for conducting them.

How is it shared?

✓ *Enhanced trust*: Face to face meetings are the most efficient way to create and sustain trust among NSIE members
✓ *Simple protocols*: An agreed distribution policy (e.g. Traffic Light Protocol) has been shown to help build trust
✓ *Extranet*: A protected extranet, usually managed by the government, may be used to disseminate information (i.e. announcements, meeting summaries, action items and even analysis reports)
✓ *Direct contacts*: As trust within the group grows, members develop informal links via telephone and/or email. Furthermore, when a network of trust has been established, an NSIE will sometimes organise conference calls to provide immediate assistance to NSIE member organizations when urgent security concerns arise.

Typical Problems

✓ The lack of national legal framework on Public Private Partnerships
✓ Immature level of information sharing culture i.e policy, regulation and co-operation with providers
✓ Improper size, profile of participants, or expertise of participating experts
✓ Poorly defined mission and scope (e.g. not having operational character, response and recovery role) of the NSIE
✓ Poor incentives to providers for participation
✓ Unbalanced sharing of information (e.g. mostly from private to public stakeholders)
✓ Continuously changing participants
✓ Regularly missing meetings on behalf of the participants
✓ Fear of building a Cartel due to privileged access to information
✓ Lack of proper Non Disclosure Agreements (NDAs)
✓ Improper treatment of confidential information.

The role of ENISA

Information sharing is a crucial element in EU efforts to enhance the resilience of public e-communication networks.
Unfortunately, there are only a few Information Sharing Exchanges in Europe.
ENISA could help MS to deploy such schemes, if interest exists.
Although it takes time and a lot of efforts in establishing and running a NSIE, Europe should take advantage of NSIEs benefits and develop national as well as pan European Information Sharing Schemes.
To accomplish this, co-operation among national initiatives and a pan European one is necessary.
In this light, the good practice guide on Information Sharing produced by ENISA helps Member States to develop knowledge and expertise in this area.

For further information visit:

ENISA’s resilience site:

https://www.enisa.europa.eu/act/res/

Full Report:

https://www.enisa.europa.eu/act/res/policies/good-practices-1/information-sharing-exchange/good-practice-guide/at_download/fullReport

Further Contact Details:

Dr. Vangelis OUZOUNIS
Senior Expert - Network Security Policies
Technical Department
ENISA
resilience-policies@enisa.europa.eu