Information Sharing Exchanges – better understand a constantly changing environment

Abstract

Information sharing among private and public stakeholder is necessary to better understand a constantly changing environment in communication networks. ENISA's stock taking and analysis revealed the importance and strategic value of partnerships among public and private stakeholders. One particular form of partnership is information sharing exchange among key stakeholders. Such partnerships are sometimes referred to as 'Network Security Information Exchanges' (NSIEs) although it is recognised that alternative names can also be used.

Today there are only a few Member States in Europe actively running an information sharing exchange. The market (e.g. providers/operators, etc.) can discuss with government and public authorities —the lessons learned from their experiences and can also share efforts and ideas with regard to a more coherent approach to crisis management and remediation planning.

Member States strongly interested in better understanding and deploying the concept of NSIE. For that reason they requested ENISA to develop a good practice guide. The main aim of this guide is to assist Member States and other relevant public stakeholders in setting up and running NSIEs. Such a guide will hopefully pave the way for an accelerated deployment of national NSIE and consequently co-operation among public and private stakeholders at pan European level.

Characteristics of 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

When you consider setting up an NSIE, it helps to understand its basic characteristics:

- *Small group*: Studies show that the most effective size of a sharing, trusting group is between 20 and 30, no more
- *Regular, face-face meetings*: Central to the effective working of the NSIE are regular, face-to-face meetings which establish trust and facilitate a free exchange of ideas
- *Government's role*: The role of government as honest broker with no commercial interests and also as the provider of threat information which is not available anywhere else is one of the critical success factors of an NSIE
- *Strategic issues*: An NSIE should address strategic issues (e.g. major/critical disruptions) rather than damage recovery
- *No participation fees*. Membership of an NSIE should be free at the point of delivery, with the only cost to members being their time and travel expenses

- *Two chairs*: Most existing NSIE's are jointly chaired by a representative from the government and a representative from industry
- *Incentives*: An NSIE should provide with incentives for members to participate i.e. save money by helping to reduce the cost of failure from incidents, reduce operational costs by learning from peers on what works and what doesn't
- *Information sensitivity*: NSIEs must recognise and respect that their members have commercial sensitivities related to the reveal of critical (i.e. weaknesses and vulnerabilities) information to competitors and / or regulators
- *Exchange vs transfer*: Emphasis is on *information exchange, not information transfer*. Normally, there should be no room for listeners and observers in a successful NSIE
- *High level security experts* usually participate in NSIES

NSIEs operate within a well-structured environment that promotes mutual trust between members. In that respect NSIEs usually perform the following tasks:

- Identify emerging threats and analyze their potential impact on public telecommunication networks
- Assess the impact of incidents (security breaches, network failures, service interruptions)
- Identify, analyse, and adopt appropriate preparedness measures to mitigate such threats and risks
- Set up procedures to continually review the implementation of adopted measures and further introduce measures of convergence when deviations observed.

What is shared and how

Information that might usefully be shared in NSIEs would include: incidents, product technical vulnerabilities and risks, protocol vulnerabilities, network intrusion information, probing attacks and network configuration issues within standards. A more detailed description of information shared in the context of an NSIE is given below:

- 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

As we have already pointed, information shared within an NSIE is sensitive and as such particular provisions must be taken in terms of how this information is 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.

Interfaces with other Bodies

An NSIE is a key part of the network security framework within a community. As such, it regularly communicates with other bodies or organizations. Such bodies might include:

- *Law Enforcement authorities*: Mixed approaches exist in terms of whether reports should be delivered to law enforcement authorities. In any case, advice should be sought at an early stage about the role of law enforcement on whether they would be able to agree to the NSIE rules on disclosure.

- *Telecommunications Regulator*: It is quite common, that the regulator is not part of the NSIE. This is due to the fact that industry members would not feel comfortable to share information of interest to telecommunications' regulator. In any case, careful consideration should be given to how the Telecommunications Regulator should or should not be directly involved in the NSIE, depending on the regulatory environment and members views.

- *Other Resilience-related bodies*: It is not usual for the NSIE to communicate directly and fully with other resilience bodies. Each country has to adapt an NSIE to its own unique political, cultural and economic circumstances.

- *Other national information sharing schemes*: Co-operation on an ad-hoc basis exists. Each country has developed its own information sharing model

- *Pan European Information sharing schemes*: Although EC tries to launch such an initiative, no pan European information sharing scheme exists for the time being. If this would be the case, then co-operation with of all national platforms is of vital importance for the enhancement of network resilience across Europe.

Typical Problems

The participation in an NSIE demands positive action and the commitment of resources on behalf of the stakeholders. On the other hand, it appears to offer intangible benefits to them, this way make them refrain from participation. Typical problems of existing NSIEs include:

- 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)
- Changing continuously 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

Conclusions

Information sharing is a crucial element in EU efforts to enhance the resilience of public e-communication networks. It helps to better understand a complex issue such as network resiliency in a constantly changing environment. 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 an Information Sharing Exchange, Europe should take advantage from 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.