A Framework for Information Sharing and Alerting

Ferenc Suba & Bence Birkas
CERT-Hungary
European Information Sharing and Alert System (EISAS)

Starting point: EISAS Feasibility Study (ENISA, 2007)

EC co-funded project

February 2009 - January 2011

Under the Programme for „Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks”

A part of the European Programme for Critical Infrastructure Protection (EPCIP)
Mission: Raising the information level and the awareness of IT security issues

Target Groups: Citizens and SMEs

Types of Information: Alerts, advisories, best practices, awareness information

Appropriate Format: Timely, trustworthy and tailored (subject of interest, less technical, in native languages)

Effective distribution of information: Multiple channels, integration of related initiatives in EU
The network which acts as a meta-information broker for alerts, advisories, best practices, awareness information in Europe
NETWORK SECURITY ORGANISATIONS (e.g. CERT TEAMS)
Every network security organisation that joined FISHA network forms a node that is an integral part of the network. It holds a web portal that provides information for final users, generates new information, increases the value of information (e.g. add best practice to alerts, translate information into other languages) or shares the information which it possesses.

LOCAL INFORMATION BROKERS
Distribution channels for information from FISHA network. Every possible way to reach the final recipient: web portals, RSS, radio, TV, awareness campaigns etc.

INFORMATION PRODUCERS
Reputable entities delivering valuable information or materials concerning security. For example software and hardware producers (e.g. MS, Secunia).

INFORMATION CONSUMERS
Members of target groups.
Core Node (to manage P2P network)

Basic Node

Target Groups
Node’s functions

Function within P2P network:

- Core node
- Basic node

Information processing:

- Creating information
- Modifying information
- Receiving information
Technical organization

- Based on hybrid-P2P
- Ordered structure - ring based
- Two kinds of nodes
- Secured communication
- Position depends on unique ID

CORE NODE

BASIC NODE
There will be a **Steering Committee** with **personalities** from the field, which publishes a policy of the “FISHA Network” (European Information Sharing and Alert System - EISAS).

**The Steering Committee decides:**
- Who can become a member of the network
- What will be its role
- Who will additionally work in the **Core Network** (offer the necessary services and responsibility)

**All participants of the FISHA Network (including the Steering Committee) will be obligated to follow the policy of the “FISHA Network”**.
- **Meta-information tagging**
  Ordered network including database of information concerning Internet security, organized based on tag system.

- **Rating system**
  Evaluation of usability of particular meta-information for every user of the FISHA network.

- **Possibility of advanced search for security information**
FISHA Action Plan

- Inventory of related initiatives
- Requirements analysis
- E-security web-portal
- System architecture & protocol
- Cooperation framework
- Communication plan
- Implementation of the system
European Information Sharing and Alert System

Home users and SMEs → a weak point in global security

Common undertaking of European network security organizations to cooperate and exchange information
A Framework for Information Sharing and Alerting in Europe

Thank you for your attention!

Questions?

Ferenc Suba & Bence Birkás

CERT-Hungary
Theodore Puskas Foundation
www.cert-hungary.hu