Minutes of the workshop on information sharing structures
NISHA closing workshop

Zürich, Switzerland

12 February, 2014

Background of the project

The 2009 Communication from the European Commission on Critical Information Infrastructure Protection[1] pointed out the importance of CIIs for the economy and the societal growth of Europe. For this reason, Member States should have a mechanism to provide information sharing, early warning and alerting capabilities for all stakeholders. The FISHA project laid down the foundations of a common European information sharing and alerting system in the form of a prototype system, based on findings of the EISAS Feasibility Study done by ENISA.

The follow-up project, NISHA builds on the results of the predecessor project, developing it into a pilot system, where the functionalities of the IT system and the usability of the outreach concept can be tested in real environment.

The NISHA project is a collaboration between NISZ National Infocommunication Service Company Ltd, NASK, FCCN, and the University of Gelsenkirchen. The project is implemented under the special European Commission Programme „Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks" (CIPS) as a part of the European Programme for Critical Infrastructure Protection (EPCIP).

With financial support from the Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks Programme European Commission - Directorate-General Home Affairs

[1] COM(2009)149 – "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience"

Minutes of the workshop

Agenda of the workshop

09.30 – 09.45 welcome, workshop objectives
09.45 – 10.15 Digital tools and services to raise awareness and promote a better internet, Hans Martens, INSAFE
10.15 - 10.35 Introducing the NISHA concept and results, NISHA consortium members
10.35 – 11.00 coffee break
11.00 – 11.45 NISHA continued
11.45 – 12.15 Information Exchange on Targeted Incidents in Practice, Freddy Dezeure, CERT-EU
12.15 - 12.30 Information Sharing Experience - The Good, the Bad and the Ugly, Alexandre Dulaunoy, CIRCL.lu
12.30 - 12.45 n6: automated network threat exchange, Piotr Kijewski, CERT.pl/NASK
12.45 – 13.00 Introducing Warden & IDEA, Pavel Kácha, CESNET
13.00 – 13.45 lunch
13.45 – 14.15 Taranis: turning your sources into reusable security alerts, Edwin Trump, NCSC.nl
14.15 - 14.45 Data exchange, Lionel Ferette, ENISA
14.45 - 15.15 MANTIS, Bernd Grobauer, Siemens CERT
15.15 – 15.30 tea break
15.30 – 15.50 discussion and conclusion
15.50 – 16.00 closing remarks

Attendance
see Annex 1

The information sharing workshop was organized along the following main objectives:

- introducing the final results of the NISHA concept: cooperation models, lessons learned, legal and organizational obstacles, possible ways to go forward
- presenting existing info sharing initiatives from general awareness raising to data & threat exchange
- addressing the barriers that exist in each presented initiatives: why these barriers exist, how they can be overcome
- trying to find synergies between the existing mechanisms
- trying to identify how one mechanism can use the info provided by the other
- trying to find where the NISHA concept/infrastructure can have an added value

The workshop was collocated with the 41st TF-CSIRT symposium, where the relevant European CSIRTs were present. The workshop intended to address the European CSIRT community, who plays an active role both in awareness raising and information sharing both in national and cross-border initiatives.

09.30 – 10.00 welcome, workshop objectives, Bence Birkas, NISZ
10.00 – 10.30 Digital tools and services to raise awareness and promote a better internet, Hans Martens, INSAFE

- Awareness center; helplines
    - Obstacles:

- Organizational organizations
- socio-economic difference
- differences in inline safety issues (issues change country by country)
- differences in awareness-raising strategies

- solutions: 4 core pillars to ensure effective and cost-efficient services:
  - Exchanging best practices
  - work with youth
  - assessments of sic activities
  - a database for more rapid take down the sites

NISHA possible contributions:
- have good source resources
- better dissemination of information/best practices
- Translation to national languages

10.30 - 11.30 Introducing the NISHA concept and results, Katarzyna Gorzelak, Bence Birkas, Michael Sparenberg

- Nisha facilitates the distribution of information to people
- Information from creators to brokers
- Translate this information to our national language.
- local nodes/portal can reach local information producers, and then disseminate the information to the network.

licensing

- obstacles
  - local blacklisting required
  - 3rd party translations and derivative works
  - referenced contend (links to external media)
  - shared ownership /copyright
  - viral license types (hindering license migrations)

- solutions
  - releases nisha soft under terms of the EUPL
  - provide content licenses: ODBC IDbl

Question: EUPL incompatible with GPL

11.45 – 12.15 Information Exchange on Targeted Incidents in Practice, Freddy Dezeure, CERT-EU

- Obstacles
  - Initial infection very difficult to avoid
  - detection more than 1 year
  - remediation: 1-6 months

information overflow
- public information
- information without context
- overload of irrelevant info

information deficit
- fear of brand image damage

- over classified
- lack of tools

circle of trust
- communities of organizations that trust each other
- sharing non-public information
- protection the information

data quality
- validated at the source
- in context

automated tools
- synchronization
- correlation

Solution

Database with indicator of compromise (IoC)
- from incidents in the constituency
- from trusted groups
- from commercial subscription
- from other information sharing

Interest to NISHA
- find a way to include the information resulting of this database in our own portal.
- Integration of this tool with NISHA

12.15 - 12.30 Information Sharing Experience - The Good, the Bad and the Ugly, Alexandre Dulaunoy, CIRCL.lu

Obstacles
- Some partners might reuse the information shared into a report and reference you as an origin of the information
- Different classification scheme in the same information sharing platform
- Indicators acquired in questionable ways
- when do you share the information

12.30 - 13.00 n6: automated network threat exchange, Piotr Kijewski, CERT.pl/NASK
- The end-user (the infected) don´t use the data. Possibly the data does not reach them.

12:45 Automated information exchange in CESNET

Warden
- Only university use their system

Obstacles
- single attacker, single target
- not extensible
- no voluntary anonymity
- no common taxonomy
- standards
- cannot usably map most of the information from external sources

IDEA Intrusion detection extensible alert to solve the problems
- keys at the same place same types

- json data model
- extensibility
- incompleteness, anonymization , spoofing
- machine parseable , human readable
- use standards

Problems: Not everybody uses standards or same taxonomy, classification.

13.45 – 14.25 Taranis: turning your sources into reusable security alerts, Edwin Trump, NCSC.nl

- based in CVE and CPE, Advisory, alerting
- XML

Benefits

- Ability to monitor more sources
- improved traceability
- automation
- ability to keep the finger on the pulse
- integration with others Taranis instances

Needs human resources: 3 full-time to Taranis.
Original information, referring original source.

Interest to NISHA:

- email features

14.25 - 15.00 Data exchange, Lionel Ferette, ENISA

- Email to exchange threats information is the most used
- Barriers to information sharing
  - Technical problems and legal problem, insufficient interest of the partners, trust issues
  - Technical issues:
    - Format changes
    - Too many formats
    - mapping of IP
    - Find contact information for IP

Recommendation:

- Security feeds providers should improve the stability of existing incident information feeds and maintain the formats
- Use of existing tools for more effective sharing of information
- A common information repository with the integration of current data exchange efforts
- local adoption of interoperable standards of data formats
- the definition of diffusion policy standards
- coordination at international level

15.30 – 16.00 MANTIS at Siemens, Tomas Schreck, Siemens CERT

- threat intelligence management
- usage of different standards such as STIX, Cybox, OpenIOC and the Mantis framework developed by Siemens for this purpose

The workshop detailed a number of information sharing mechanisms that deal with different layers of

data. The notes of the workshop include various aspects on how the given information sharing mechanisms could be of use for the NISHA concept, but coming up with a structured list of observations was not possible due to lack of time. Four questions were drafted for discussion to learn more about the points of views of the participants:

- What do you find the biggest challenge in information sharing at your organization?
- Do you think CERTs should focus more on general awareness raising? How to engage more with the awareness raising community?
- Do you think discussion on information sharing problems raised by the workshop should be continued? In what form?
- What important aspect of information sharing was missed out today?

To gain a better understanding of the various perspectives, a questionnaire will be sent to the workshop participants as a follow-up of the event to draw appropriate conclusions.

The presentations of the workshop will be available for download at www.nisha-network.eu.

Annex 1.

List of participants

1.	Alexandre EPINAT	BNP PARIBAS CSIRT Group	France
2.	Steve GIRAUD	BNP PARIBAS CSIRT Group	France
3.	Gyebrovszki Tamás	GovCERT-Hungary	Hungary
4.	Szép Tamás	GovCERT-Hungary	Hungary
5.	Pavel Kácha	CESNET	Czech Republic
6.	Andrea Kropacova	CESNET	Czech Republic
7.	Daniel Roethlisberger	SWITCH-CERT	Switzerland
8.	Monika Josi	Microsoft Corporation/CH	Switzerland
9.	Kauto Huopio	NCSC-FI	Finland
10.	Hideo Kinoshita	MUFG-CERT	Japan
11.	Tatsuya Kitao	MUFG-CERT	Japan
12.	Lionel Ferette	ENISA	Europe
13.	Thomas Schreck	Siemens CERT	Germany
14.	Valeriu Vraciu	Ro-CSIRT	Romania
15.	Alexander Jaeger	BASF CERT	Germany
16.	Hans Martens	INSAFE	Belguim
17.	Edvin Tump	NCSC.nl	The Netherlands
18.	Bob van der Kamp	NCSC.nl	The Netherlands
19.	Francesco Lapa	CERT Poste Italiane	Italy
20.	Freddy Dezeure	CERT-EU	Europe
21.	Alexandre Dulaunoy	CIRCL.lu	Luxembourg
22.	Antonio Merola	CERT Poste Italiane	Italy
23.	Piotr Kijewski	NASK	Poland
24.	Katarzyna Gorzelak	NASK	Poland
25.	Bence Birkas	NISZ Ltd	Hungary
26.	Michael Sparenberg	Westfachlische Hochschule	Germany
27.	Jorge de Carvalho	FCT	Portugal
28.	Timo Mischitz	GovCERT.at	Austria
29.	Masato Terada	Hitachi CERT	Japan
30.	Johannes Clos	CERT Bund	Germany
31.	Jeroen Massar		Switzerland
32.	Christopher Fischer	BFK	Germany
33.	Spinu Natalia	CERT.Gov-MD	Moldova
34.	Erika Stockinger	CERT-SE	Sweden
35.	Raphael Vinot	CIRCL.lu	Luxembourg
36.	Bernd Grobauer	Siemens CERT	Germany