



28.12.2006

ITT
Jarkko Saarimäki

Framework for Vulnerability Information Sharing



28.12.2006

Finnish Communications Regulatory Authority / CERT-FI Framework for Vulnerability Information Sharing

Introduction

What is CERT-FI

CERT activities mean prevention, observation and solution of information security violations and information on threats to information security. CERT is an abbreviation of Computer Emergency Response Team. There are several CERT organisations all over the world. They co-operate with each other and distribute information on information security threats and related matters and inform the users of systems e.g. via the Internet. The main goal of CERT activities could be to prevent and control the violations of and threats to the data in information systems as objectively and efficiently as possible.

In FICORA, the group focused on information security incidents and their control is called CERT-FI (Computer Emergency Response Team FICORA). In its activities, it tries to implement the principles of overall CERT activities and to promote security in the information society. CERT-FI cooperates with national and international CERT actors and representatives of trade and industry and public administration. FICORA also coordinates a CERT working group, which acts as a cooperative body for different actors in the field of observation and solution of information security incidents. This working group also follows up and promotes the general evolution in the field and knowledge of it.

CERT-FI receives the notifications of telecommunications operators concerning information security incidents and threats. In addition, the CERT-FI group of FICORA continuously follows up worldwide the current events in the information security, security problems of information systems and security incidents and response to them. The duties of CERT-FI are among other things:

- to implement nationwide monitoring of incidents, documentation and statistics
- to make and maintain an estimation of information security threats and to inform of observations
- to give recommendations, advice and guidelines for improvement of information security
- to diffuse information for the prevention of information security violations
- to help solving information security problems
- to cooperate with suppliers of equipment, networks and software
- to be contact with the Police and other authorities and to coordinate the cooperation in information security
- to follow up and analyse international and other development related to information security threats
- to maintain international contacts between authorities in CERT activities

This framework is intended to help CERT-FI and commercial organizations to work in partnership to coordinate vulnerability information handling. By adhering to this framework you will be part of a mechanism through which technical and commercial vulnerability information can be shared between partners. This Framework is intended to increase the flow of vulnerability information within a trusted environment whereby issues can be solved quickly and easily, while at the same time limiting the likelihood of uncontrolled public release.

This is not a legal contract. It is a clear statement about the requirements for information sharing between CERT-FI and the receiving organization.



28.12.2006

The Traffic Light Protocol - TLP

CERT-FI has agreed to a labelling mechanism known as the "Traffic Light Protocol" (TLP). This same protocol has now been accepted as a model for trusted information exchange by over 30 other countries. The protocol provides for four "information sharing levels" for the handling of sensitive information. The four information sharing levels are:

- RED - Personal for named recipients only. In the context of a meeting, for example, RED information is limited to those present. In most circumstances RED information will be passed verbally or in person.
- AMBER - Limited distribution. The recipient may share AMBER information with others within their organization, but only on a "need-to-know" basis.
- GREEN - Community wide. Information in this category can be circulated widely within a particular community. However, the information may not be published or posted on the Internet, nor released outside of the community.
- WHITE - Unlimited. Subject to standard copyright rules, WHITE information may be distributed freely, without restriction.

The TLP has compatibility issues with Finnish legislative environment. Under Finnish Law, there is a possibility that TLP-marked information could be released beyond its intended circulation. This unintended distribution may be prevented by adding a Finnish classification when this can be done in accordance with Finnish law.

Framework for the exchange of Vulnerability Information FICORA/CERT-FI and the receiving company agree to:

1. label vulnerability information to be shared with one of the four "information sharing levels" identified in the Traffic Light Protocol (TLP);
2. where necessary and appropriate to protectively mark the information in line with their internal security policies and in accordance with TLP;
3. use the same degree of care to maintain confidentiality of vulnerability information exchanged as for their own commercially sensitive information;
4. not directly or indirectly disclose the agreed public disclosure date, existence of, or details pertaining to, vulnerability information to a third party without the prior written approval of the originating organization;
5. not use the vulnerability information disclosed for commercial advantage or marketing purposes;
6. control the release of vulnerability information solely to those employees that have a need to know as an aspect of their job or role. Such persons must be appropriately briefed on, and bound by the meaning of the TLP sharing mechanism;
7. advise each employee, before he or she receives access to vulnerability information, of its confidential nature and the requirements to protect it in line with internal policies;
8. destroy vulnerability information that is no longer required;
9. disclaim liability for any damages arising out of the use of the information and access to it is offered without financial charge or warranties of any kind;
10. not employ legal remedies to address any conflicts resulting from the disclosure or use of vulnerability information.