

Role of the **Vulnerability Coordinators**

2009-03-31
Brussels

Erka Koivunen
Head of CERT-FI
Finnish Communications
Regulatory Authority



Vulnerability Coordinators' Playing Field

Reactive Services	Proactive Services	Artifact Handling
<p>Alerts and Warnings</p> <p>Incident Handling</p> <ul style="list-style-type: none"> • Incident analysis • Incident response support • Incident response coordination • Incident response on site <p>Vulnerability Handling</p> <ul style="list-style-type: none"> • Vulnerability analysis • Vulnerability response • <u>Vulnerability response coordination</u> 	<p>Announcements</p> <p>Technology Watch</p> <p>Security Audits or Assessments</p> <p>Configuration and Maintenance of Security Tools, Applications, and Infrastructures</p> <p>Development of Security Tools</p> <p>Intrusion Detection Services</p> <p>Security-Related Information Dissemination</p>	<ul style="list-style-type: none"> • Artifact analysis • Artifact response • Artifact response coordination <p>Security Quality Management</p> <p>Risk Analysis</p> <p>Business Continuity and Disaster Recovery</p> <p>Security Consulting</p> <p>Awareness Building</p> <p>Education/Training</p> <p>Product Evaluation or Certification</p>

CERT/CC: CSIRT Services

ENISA: A Step-by-Step approach on how to set up a CSIRT

Ideally, we don't need coordinators.

And if they are needed, the less coordinators are involved in any given project the better.



Minding one's own Business vs. Saving the World?



- Are Finnish interests threatened?
- Can we be of help to others?
- Is the problem bigger than we can handle?

DISCOVERY



- vulnerability discovered
- finder decides to offer for coordination

INITIATE COORDINATION



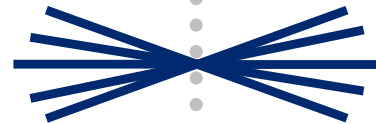
- decision to accept coordination task

REMEDIATION



- approaching (most likely) affected vendors
- agreeing on non-disclosure and administrative issues
- disclosing material to participating vendors
- supporting participating vendors
- handling public relations

EARLY-WARNING



- disseminating early-warning information

DISCLOSURE



- fix release
- advisory release
- handling public relations



Q: How CERT-FI got
Involved?

A:



- | Projects | year of disclosure |
|--------------------------------|--------------------|
| • ISAKMP | 2005 |
| • Archive Formats | 2008 |
| • SSL | 2008 |
| • TCP | <i>[ongoing]</i> |
| • <i>[yet-to-be-disclosed]</i> | <i>[ongoing]</i> |

- Multi-Vendor coordination
 - Level of Awareness and Disclosure Strategies varies
- Logistics of mass deployments
- Dissemination of Early Warning Information
 - Pronounced need of secrecy implies lack of trust
- Industries with no change management culture
 - read: SCADA
- Resourcing and funding



Recommendations for a Way Forward

- National (and trustworthy) Points of Contact (CERTs?)
 - Sharing of early warning information on vulnerabilities
 - Localised impact assessment
 - Helping domestic vendors cope with the issues
- Raising the bar among industry
 - Incentives vs. Liabilities?
- Research
 - Complement efforts such as NIST/NVD of US
 - Testing methodology, securing complex systems, secure programming..

National **EMERGENCY SUPPLY** Agency
Co-operation for the protection of critical systems

Telephone: +358 9 6966 510

E-mail: cert@ficora.fi

WWW: www.cert.fi

**CERT-FI alerts and advisories are
available in Finnish via:**

- E-mail
- SMS (subscription fees apply)
- web pages
- RSS feed
- TELETEXT page 848 (YLE)