

eCSIRT.net The European CSIRT Network

Olaf Gellert
Don Stikvoort
Klaus-Peter Kossakowski



© 2000-2002 by PRESECURE® Consulting GmbH

Problem Statement

- **No education path for „Incident Handler“**
 - „Training on the job“ is *unbezahlbar*
- **Slow progress on standards for „Incident Handler“**
 - Teams need to become „smarter“
 - Lack of support by tools, interface, knowledge bases
- **Strategical weaknesses**
 - Centralized teams cannot address local issues
 - „Manual reporting“ often translate to „No reporting“
- **Legal issues**
 - Forensics
 - International incidents



Slide 2 / TF-CSIRT - May 2002
© 2000-2002 by PRESECURE® Consulting GmbH

Concentrate on one Problem

- No education path for „Incident Handler“
 - „Training on the job“ is *unbezahlbar*
- **Slow progress on standards for „Incident Handler“**
 - Teams need to become „smarter“
 - Lack of support by tools, interface, knowledge bases
- **Strategical weaknesses**
 - Centralized teams cannot address local issues
 - „Manual reporting“ often translate to „No reporting“
- **Legal issues**
 - Forensics
 - International incidents



Slide 3 / TF-CSIRT – May 2002
© 2000-2002 by PRESECURE® Consulting GmbH

eCSIRT.net

- **Foundations:**
 - TI – Level 2 teams
 - build backbone for pragmatic Trial
 - IODEF / IDMEF
 - available exchange formats
- **Goals:**
 - Improve – Exchange of incident related data
 - Add – Collection / Analysis of shared data
 - Enable – Efficient cooperation



Slide 4 / TF-CSIRT – May 2002
© 2000-2002 by PRESECURE® Consulting GmbH

eCSIRT.net - Participants

- | | |
|-----------------------------|-----------------|
| ■ CERT-POLSKA / NASK | Poland |
| ■ DFN-CERT | Germany |
| ■ DK-CERT / UNI-C | Denmark |
| ■ GARRNET-CERT / INFN | Italy |
| ■ IRIS-CERT / CISC | Spain |
| ■ JANET-CERT / UKERNA | United Kingdom |
| ■ Le CERT Renater | France |
| ■ M&I/STELVIO bv | The Netherlands |
| ■ PRESECURE Consulting GmbH | Germany |



Slide 5 / TF-CSIRT - May 2002
© 2000-2002 by PRESECURE® Consulting GmbH

Efficient Cooperation

- **By Semantics** – standardized and unambiguous
 - Statistics
 - Shared Knowledge Base
 - Trend analysis, Warnings and Alerts
- **By Services**
 - Managing the process
 - Maintaining Information Services
 - Providing Distribution Functions
 - including „out-of-Internet“ alerting



Slide 6 / TF-CSIRT - May 2002
© 2000-2002 by PRESECURE® Consulting GmbH

Technical Working Packages

■ Initialisation (2002)

- WP2: Preparation Phase

■ Trial (2002-2003)

- WP3: Usage Phase (2002-2003)
- WP4: Clearinghouse Function (2003)
- WP5: Alert Function (2003)



Slide 7 / TF-CSIRT - May 2002
© 2000-2002 by PRESECURE® Consulting GmbH

WP2: „Defining a common language“

This addresses the specification, adaptation and integration of available techniques, and the development of a necessary common framework, to enable and facilitate the work under wp 3, 4 and 5.

- Documentation of a common language (semantics) for incident data storage and exchange based on IODEF/IDMEF (syntac)
- Documentation on the integration of common language into CSIRT operation
- Guideline "How to apply common language "
- Code of Conduct supported by partners
- Overview of IODEF /IDMEF enabled/capable solutions available to CSIRT



Slide 8 / TF-CSIRT - May 2002
© 2000-2002 by PRESECURE® Consulting GmbH

WP3: „using the common language“

The usage phase is based on the established common framework and covers the actual usage of identified solutions.

- Progress reports on the usage and experiences with the solutions applied
- Updates on the solutions/products list of WP 2
- Updates on the guideline of WP 2
- Final report on the results of the usage within the partner environments



Slide 9 / TF-CSIRT – May 2002
© 2000-2002 by PRESECURE® Consulting GmbH

WP4: „gathering incident statistics“

The Clearinghouse Function builds on the established common framework to collect incident statistics partners and serve these in an integrated fashion to the partners, and – in a generalized way – to a wider audience.

- Clearinghouse policy
- Aggregated generalized statistics suitable for a wider audience
- Collection of sanitized case and success stories for a wider audience, based on partner input
- Individual and aggregated statistics of partner CSIRTs
- References to public statistics of CSIRTs



Slide 10 / TF-CSIRT – May 2002
© 2000-2002 by PRESECURE® Consulting GmbH

WP5: „gathering incident data to derive early warnings and emergency alerts“

The Alert Function builds on the established common framework to collect incident data and then deploy techniques to intelligently combine these to yield early warning information, in the form of warnings or emergency alerts to the partners.

- Alert Policy
- Specified and established techniques for in-band Internet based alerting
- Specified and established techniques for “out-of-band” (not Internet based) alerting
- Warnings and alerts that go out to the partners, providing sufficient input



Slide 11 / TF-CSIRT – May 2002
© 2000-2002 by PRESECURE® Consulting GmbH

WP5: Alert Function - Clarifications

- **For the spreading of warnings and alerts suitable techniques will be adopted:**
 - in-band (using the Internet) or
 - out-of-band (not the Internet) – leaning on infrastructures available/developed elsewhere
- **Liaisons with international bodies that**
 - agree to the rules governing the alert function
 - can contribute alert information during European “out-of-hours” time periods



Slide 12 / TF-CSIRT – May 2002
© 2000-2002 by PRESECURE® Consulting GmbH

Exploitation

- **Project partners play an active role in advancing the state of the art**
 - Contributions to FIRST, TF-CSIRT, ...
- **eCSIRT.net public web site**
 - Building public awareness
 - Online dissemination information
- **eCSIRT.net user group**
 - Restricted web site
- **Publications and presentations**
- **Clustering with EC projects**



Slide 13 / TF-CSIRT - May 2002
© 2000-2002 by PRESECURE® Consulting GmbH

Innovation of eCSIRT.net

Enhancing

- performance of CSIRTs
- cooperation amongst CSIRTs

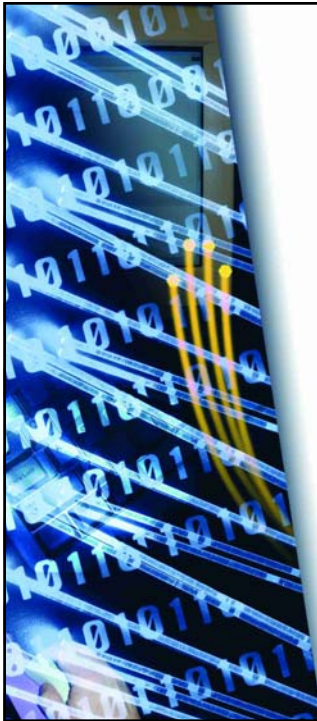
Facilitating

- information dissemination amongst CSIRTs
- availability of early warning information to CSIRTs
- availability of value added information in and outside CSIRTs
 - analysis and assessment in terms of statistics
 - best practices to avoid incidents

Establishing the basis for adoption of new Technologies as new best practice



Slide 14 / TF-CSIRT - May 2002
© 2000-2002 by PRESECURE® Consulting GmbH



Thank
you!



© 2000-2002 by PRESECURE® Consulting GmbH

Scientific Coordinator

Dr. Klaus-Peter Kossakowski

WWW: <https://www.pre-secure.de>
 <https://www.pre-secure.com>

Email: kpk@pre-secure.de

Mobil: (+49) 0171 / 5767010