



eCSIRT.net The European CSIRT Network

**Supporting the
CSIRT Infrastructure**

Klaus-Peter Kossakowski

© 2000-2003 by PRESECURE® Consulting GmbH



Update on current activities

- IODEF and common language not covered here → Presentation by Jan Meijer
- Code of Conduct
- Clearinghouse (aka Statistic) Function
- Alert Function

Slide 2

© 2000-2003 by PRESECURE® Consulting GmbH



The Code-of-Conduct is ready ...

- Co-operation is voluntary and can be terminated at any time.
- Co-operation [...] will not infringe on partners business.
- Information and intellectual property rights [...] must be protected.
- Confidentiality of constituent data will be given highest priority.
- Services provided by the partners should steadily improve.
- Policies, procedures and workflows [...] should be optimized by the exchange of knowledge and practice [...].
- The partners will develop and enable means for an improved exchange of knowledge and practices and will provide training material.
- The work and co-operation of partners should set an example for other CSIRTs and should provide a model for similar initiatives around the world.



Slide 3

© 2000-2003 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 4

© 2000-2003 by PRESECURE® Consulting GmbH

Use of the Clearinghouse Function

- **As much information as legally can be shared**
 - Low priority, off-line activities
 - Incidents should be closed before they are processed for statistical purposes
- **Output is tailored towards different needs**
 - **PUBLIC:** output is shared with the public but restricted
 - **INTERNAL:** output is shared with participating CSIRTs



Slide 5

© 2000-2003 by PRESECURE® Consulting GmbH

Participation

- **Participation is restricted to teams that either are:**
 - Partner of the eCSIRT.net project
 - Liaisons of the eCSIRT.net project
- **furthermore**
 - The Code-of-Conduct must be signed
 - The Clearinghouse Policy must be accepted



Slide 6

© 2000-2003 by PRESECURE® Consulting GmbH

Type 1 Statistics

■ Meta Information on CERT workload:

- Either a product of human assessment or
- derived from tracking data by IH tools
- Data points:
 - number of reported incidents / false reports
 - number of analyzed reports and systems
 - number of attacks
 - number of affected systems, persons, organizations
 - number of attacked systems, persons, organizations
 - number of cooperating teams and manufacturers
 - time spent for support of the constituency
 - time spent for analyzing
 - time spent for documentation
 - time spent for conservation of evidence



Slide 7

© 2000-2003 by PRESECURE® Consulting GmbH

Type 2 Statistics

■ Information on Incidents handled by CERTs:

- Information sanitized by submitting CERT whenever an incident is closed
- Information submitted based on IODEF including authenticity and confidentiality
- Information collected and aggregated automatically
- Access of participating CSIRTs to aggregated data
- Subset of aggregated data as public available statistics



Slide 8

© 2000-2003 by PRESECURE® Consulting GmbH

Type 3 Statistics

■ Information on Events on the Internet:

- Not necessarily handled by a CERT
- Not necessarily a successful intrusion
- Submission ensures authenticity (and confidentiality)
- Gathered and aggregated automatically
- Access of participating CSIRTs to aggregated data
- Subset of aggregated data as public available statistics



Slide 9

© 2000-2003 by PRESECURE® Consulting GmbH

Type 3 Statistics (Techniques)

- Maintain otherwise not used system(s) reachable over the Internet
- Configuration of detection software based on CD-ROM and pregenerated public key pair
 - PRELUDE – (network) IDS, SNORT rules
 - ARGUS – monitoring (IP headers **only**)
- Reporting to central IDS manager operated by eCSIRT.net
- Access via https and user certificates



Slide 10

© 2000-2003 by PRESECURE® Consulting GmbH

Outlook for Clearinghouse Function

■ Type 2 Statistics highly controversial

- Integration of sanitizing into IH tool
- Establish „trusted third party“ to act as a clearinghouse to
 - provide better results
 - gain more acceptance

■ Future potential

- Online processing of Type 3 Statistics to generate alerts that are then communicated by the Alert Function



Slide 11

© 2000-2003 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 12

© 2000-2003 by PRESECURE® Consulting GmbH

Use of the Alert Function

- Only when there is a legitimate interest of the participating CSIRTs
- Only if the impact can be foreseen and represents a widespread threat
 - e.g. nationwide or international
- The out-of-band function shall be used only
 - If the in-band function isn't available
 - Maybe outside business hours
 - Last resort if no other communication means are available



Slide 13

© 2000-2003 by PRESECURE® Consulting GmbH

Participation

- Participation is restricted to teams that either are:
 - Partner of the eCSIRT.net project
 - Liaisons of the eCSIRT.net project
 - TI accredited teams
- furthermore
 - The Code-of-Conduct must be signed
 - The Alert Policy must be accepted



Slide 14

© 2000-2003 by PRESECURE® Consulting GmbH

Requirements - 1

- Each team must provide a functional email address
- Each team must provide a functional telephone number
- The correctness should be ensured either by
 - TI accreditation framework
 - eCSIRT project management



Slide 15

© 2000-2003 by PRESECURE® Consulting GmbH

Requirements - 2

- Each team must support cryptographic techniques based on OpenPGP and/or S/MIME standards
- The correctness of keys or certificates should be ensured either by
 - TI accreditation framework and it's formal key signing effort
 - eCSIRT project management



Slide 16

© 2000-2003 by PRESECURE® Consulting GmbH

Information Exchange Issues

■ The answers to the following questions are most important:

- Is it a new threat?
- Which vulnerabilities were used?
- What modus operandi were taken by the attackers?
- Where is the origin/source of the attack(s)?
- How can attempted attacks be detected or successful attacks be recognized?



Slide 17

© 2000-2003 by PRESECURE® Consulting GmbH

Information Exchange Issues - 2

■ Verification

- great care needs to be taken to avoid false alarms, therefore
- Only reliable information should be used
- Might come from
 - own knowledge (e.g. IDS)
 - the constituency
 - reliable and trustworthy partners



Slide 18

© 2000-2003 by PRESECURE® Consulting GmbH

Information Exchange Issues - 3

■ Internet based communication

- By email
- Format: tailored incident reporting form
 - Predefined and tailored reporting
 - Subset of the IODEF Incident Handling Profile

■ Out-of-band communication

- By telephone
- No format specified, but ...
 - English
 - Concise
 - Informative etc. etc. :)



Slide 19

© 2000-2003 by PRESECURE® Consulting GmbH

Information Exchange Issues - 4

■ Privacy and Disclosure

- Alerts should not contain
 - private information about users and sites
 - embarrassing information

■ Usage

- Alerts should be ready for use to warn the own constituency
- Alerts might initiate co-operation among the teams to formulate a proper response and to answer open questions.



Slide 20

© 2000-2003 by PRESECURE® Consulting GmbH

In-Band (Internet based) Alert Function

■ Mailing List and Security Gateway

- Linux based system
 - antivirus software
- GNU Mailman
- SecureMail Gateway (T/Bone - commercial software)
 - operates as a proxy-server
 - automatic decryption and encryption
 - supports S/MIME and PGP/GPG
 - key management
 - central security policy



Slide 21

© 2000-2003 by PRESECURE® Consulting GmbH

Out-of-the-Internet Alert Function

■ Telecommunications application server

- Automatic call processing
- Linux based server (isolated!)
- GNU Bayonne
- Up to 60 ISDN lines (starting with two :-)
- Caller identification with UID and PIN



Slide 22

© 2000-2003 by PRESECURE® Consulting GmbH

Outlook for the Alert Function

■ Further out-of-the-Internet services:

- Support of SMS
- Automatic FAX exploder to allow transfer larger documents

■ Include teams from other areas:

- Live reports from other time zones
- Early warning during out-of-hours in Europe

■ Continuity:

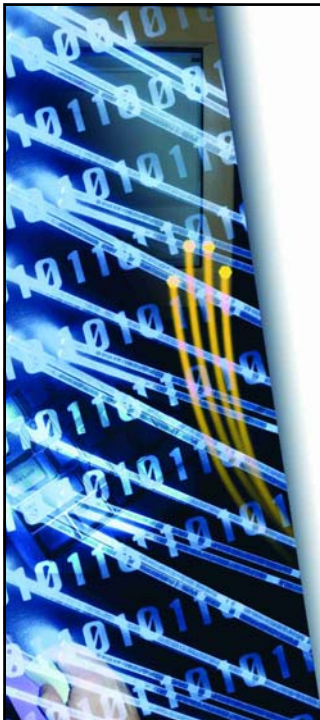
- Extend service (hardware, lines, backup)
- Funding for running costs



Slide 23

© 2000-2003 by PRESECURE® Consulting GmbH

Thank
you!



© 2000-2003 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

Slide 25

© 2000-2003 by PRESECURE® Consulting GmbH

