Automatic Exchange of incident related data – and its application in CSIRT Operations

Dr. Klaus-Peter Kossakowski for the eCSIRT.net consortium,
kpk@presecure.de / https://www.eCSIRT.net

Background

The participiants of the eCSIRT.net project have received funding from the Commission of the European Community to proof the benefits of CSIRT-to-CSIRT co-operation. The partners are co-operating in the field of incident handling and are establishing the necessary pre-requisites to build a stronger community like a Code of Conduct and procedural as well as technical guidelines. The take-up of techniques that are proposed within the project will enable the establishment of new best practices and serve the following goals:

1. to enable a standardised and unambigous exchange of incident related information between the CSIRTs involved;
2. to enable the collection of standardised and unambigous incident statistics serving CSIRTs involved and in a generalised fashion, the public;
3. to enable the collection of standardised and unambigous incident related data. This will be followed by intelligent generation of warnings and emergency alerts serving the CSIRTs involved.

The eCSIRT.net initiative is open for participation by all European teams that have been shown to follow established best practices by joining the TI accreditation framework (http://www.trusted-introducer.org). Teams outside Europe are welcome to liaise with eCSIRT.net and participate in discussions to progress the goals described above, so they can be implemented internationally. This will also progress the methods and practices developed so they can be utilized and applied in other settings.

The presentation during the FIRST 2003 conference will not focus on the project and its goals but will review existing approaches and solutions to automatically exchange incident related data among CSIRTs or receiving incident related data from constituents by CSIRTs. (Similar approaches for vulnerability related data exist but are not within the scope of this paper.)

Problem Statement

The public presentation of incidents and vulnerabilities might be seen as something that will undermine the public confidence. But it needs to be recognized that the public confidence is already heavily impacted by the headlines regarding Code Red, Nimda or the new SNMP vulnerability. All three incidents are examples for global problems not restricted to a smaller set of organizations or directed towards a particular target but attacking the community at large. In the opposite, the availability of “true” information will result in a better understanding, and only if understanding leads to an improved security culture will users and organizations know that they need to take much better proactive steps to avoid incidents and not suffer from break-ins.

Today's foundation of the distributed network of CSIRTs existing in Europe can be described as follows:

- **Established communication:** Based on Internet-based email only. Telephone and telefax might be used to confirm specific information or to discuss potential approaches.
- **No backup for Internet-based email.**
- **Established communication security:** Based on PGP encryption and digital signatures. Keys are authenticated on an ad-hoc basis through CSIRT-to-CSIRT communication.
- **No key infrastructure.**
- **Established informal knowledge-transfer:** If events are of enough interest or seem to be important, they might be shared with other teams.
- **No guidelines or requirements what should be shared with whom.**
- **Supported integration of new entities:** New CSIRTs are presented to the community by means of the European CSIRT Directory (TI, http://www.ti.terena.nl), for other areas of our global communities such directories are missing.
- **No formal integration of new CSIRTs.** No efforts are made to formally introduce new teams, although each team is welcome to sign up for accreditation under the TI framework.
- **Successful cooperation on case by case basis:** CSIRTs involved with the same incidents will share information based on a case by case basis and on the need to know principle.
- **No predetermined rules for cooperation on a routine basis.**
- **Limited availability of statistical or trend analysis outside the CSIRT community:** While value added information is available to single and cooperating teams it is rarely made available outside the CSIRT community.
- **No availability of early warning information.**
- **No established way of providing sanitized information to the public.**

The eCSIRT.net project aims to address – directly and indirectly – the recognized limitations and missing benefits of an established CSIRT infrastructure. By concentrating on the CSIRT-to-CSIRT communication and cooperation, an overall improvement for all participating CSIRTs can be achieved in regard to various aspect. The innovation is not only related to specific new technology but to new solutions to existing problems and new operational practices, but this paper will concentrate on three areas, that are approached via technical solutions that can be utilized in the environment of other CSIRTs as well:

1. **Improved communication:** By applying new established protocols – namely IODEF and IDMEF[1] – communication will be formalized and integrated into the internal workflows enable semi-automated handling of new incoming reports

---

[1] IODEF is developed within the TERENA Task Force "CSIRTs in Europe" and further extensions will be developed within the IETF INCH Working Group. IDMEF is one of the outcomes of the Intrusion Detection Working Group within the IETF.

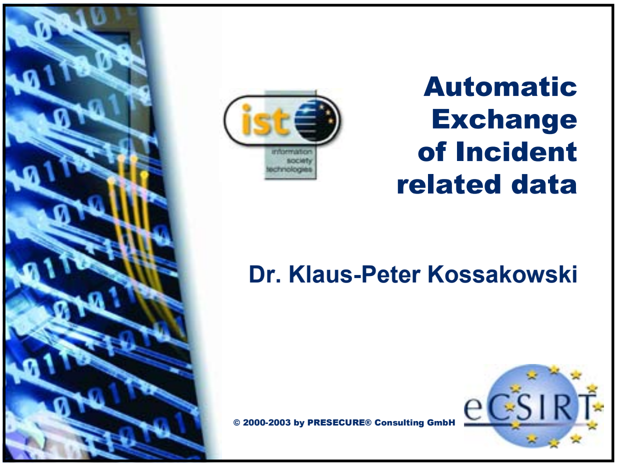
and facilitate complete and timely reporting to other CSIRTs. One side effect will be that a common language for CSIRTs will be established to describe events and data of common interest. While the protocols implement a technical and syntax oriented solution, the integration into workflows demand a semantical solution to avoid, that the same set of data exchanged is interpreted differently from the CSIRTs involved.

2. **Sanitized insights into the CSIRT community through public statistical and trend analysis:** While there is a clear need for confidentiality and privacy related to incidents, the silence about incidents, attack and their impact on the organizations as well as the society at large is not helpful. Based on the established common language necessary for the improved exchange of incident / attack related data, all events are already labeled in a standardized way. Thereby the presentation of statistical analysis is made possible without additional effort, as today any analysis would require to transform all data towards a common language first. The availability of any statistical and trend analysis is important for the teams, as they will gain arguments to support their position and services. In addition they will gain insights into their own work which would allow them to adjust their work accordingly to new trends. Without real insights which are available outside the CSIRT community the threats cannot be evaluated nor addressed on the policy level.
3. **Backup for Internet-based communication especially in regard to alerts:** While all incidents and attacks are important to the impacted users and organizations, the need for 24 by 7 (round the clock) helpdesks and service offerings are still rare. But global attacks like Nimda, Code Red or vulnerabilities like the SNMP weaknesses require immediate attention and at least the timely dissemination of heads-up and alert messages. As it is clear from the past experiences that the network itself will be impacted, backup for Internet-based communication is mandatory to allow CSIRT-to-CSIRT-communication during crisises.

The presentation attached concentrates on the integration into the CSIRT operation for the three topics listed above. All documentation related to the eCSIRT.net project – current and future – is or will be available from the web site: https://www.eCSIRT.net

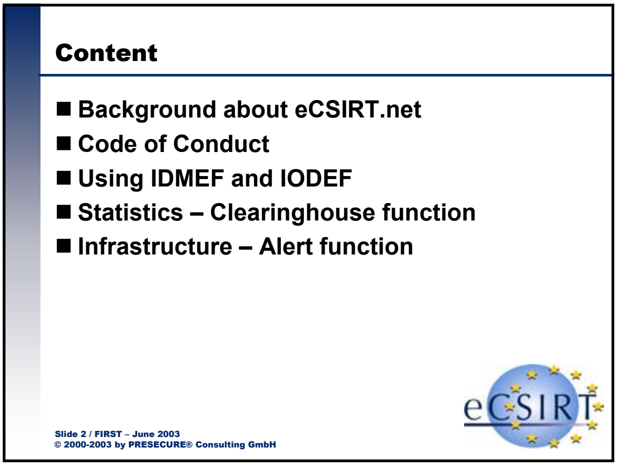
Closing Remarks

As the strength of CSIRTs lays in the close relationship between the CSIRT and their constituency, the eCSIRT.net project does not intervene in this regard. Only the information that steams from the cooperation within the CSIRT network which is especially created to support the take-up by other CSIRTs or which are “products” like the public statistics and trend analysis will be made available. Everything else will benefit the CSIRTs participating in this project – and others adopting our approach – by improving their operation and ultimately their service to their constituents. This approach will also address the recognized need to provide local support in terms of language, laws and culture.



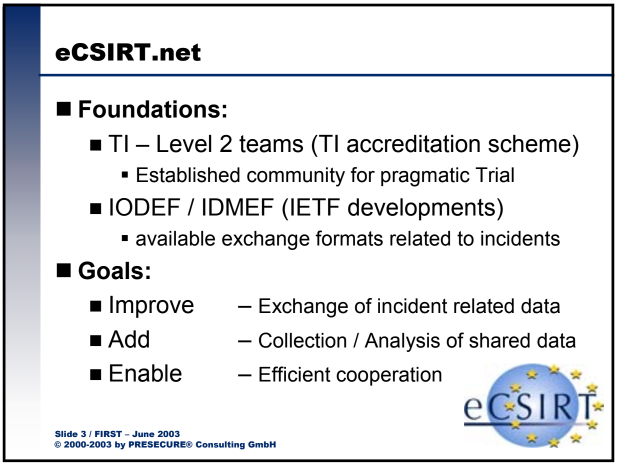
Automatic Exchange of Incident related data

Dr. Klaus-Peter Kossakowski



Content

- Background about eCSIRT.net
- Code of Conduct
- Using IDMEF and IODEF
- Statistics – Clearinghouse function
- Infrastructure – Alert function



eCSIRT.net

- **Foundations:**
  - TI – Level 2 teams (TI accreditation scheme)
    - Established community for pragmatic Trial
  - IODEF / IDMEF (IETF developments)
    - available exchange formats related to incidents
- **Goals:**
  - Improve – Exchange of incident related data
  - Add – Collection / Analysis of shared data
  - Enable – Efficient cooperation

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
STELVIO bv	The Netherlands
PRESECURE Consulting GmbH	Germany

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

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 (syntax)
- 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

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.**

WP3: „Using the common language“

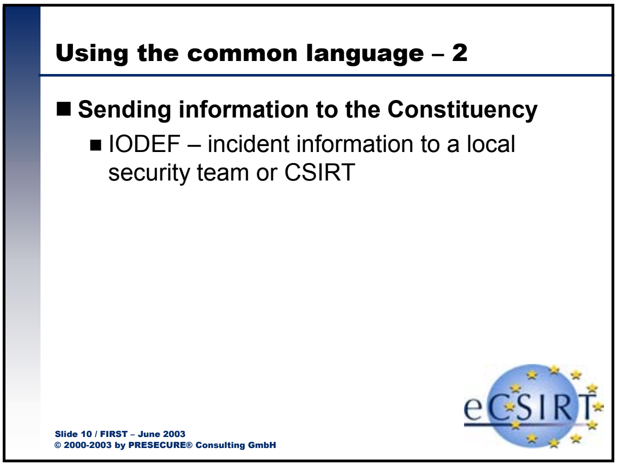
The usage phase is based on the established common framework and covers the actual usage of identified solutions.

- 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

---

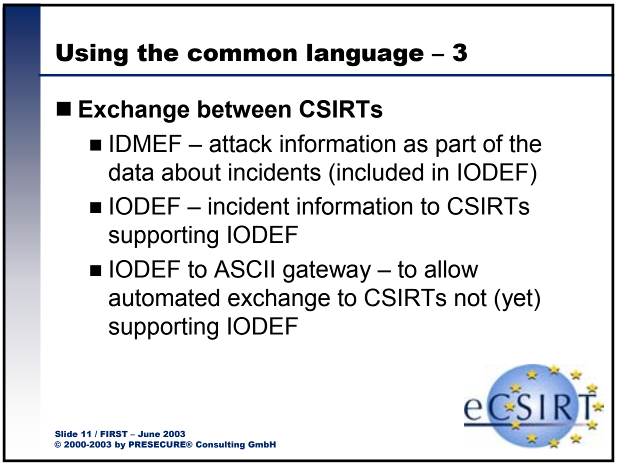
Using the common language

- **Reporting from the Constituency**
  - IDMEF – attack information directly from the sensor → AirCERT
  - IODEF – incident information from a local security team or CSIRT
  - Web based form to allow constituents to send IODEF objects



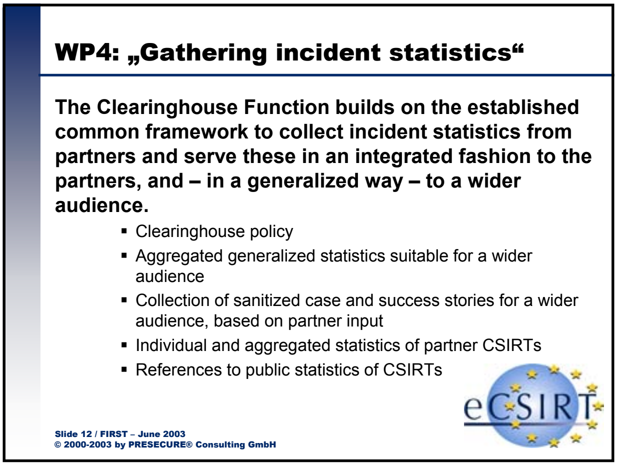
Using the common language – 2

- Sending information to the Constituency
  - IODEF – incident information to a local security team or CSIRT



Using the common language – 3

- Exchange between CSIRTs
  - IDMEF – attack information as part of the data about incidents (included in IODEF)
  - IODEF – incident information to CSIRTs supporting IODEF
  - IODEF to ASCII gateway – to allow automated exchange to CSIRTs not (yet) supporting IODEF



WP4: „Gathering incident statistics“

The Clearinghouse Function builds on the established common framework to collect incident statistics from 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

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

Participation

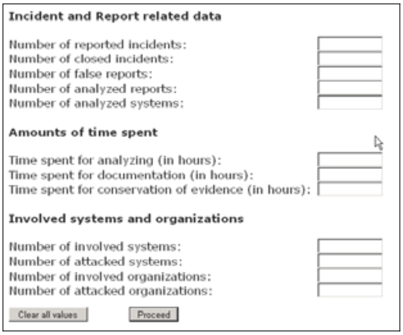
- **Participation is restricted to teams that either are:**
  - Partner of the eCSIRT.net project
  - Liaisons of the eCSIRT.net project

- **furthermore**
  - The Code-of-Conduct must be signed
  - The Clearinghouse Policy must be accepted

Type 1 Statistics

- **Meta Information on CERT workload:**
  - Either a product of human assessment or
  - derived from tracking data by IH tools
  - Characteristic 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

Type 1 Statistics – Monthly and simple



Incident and Report related data

Number of reported incidents:
Number of closed incidents:
Number of false reports:
Number of analyzed reports:
Number of analyzed systems:

Amounts of time spent

Time spent for analyzing (in hours):
Time spent for documentation (in hours):
Time spent for conservation of evidence (in hours):

Involved systems and organizations

Number of involved systems:
Number of attacked systems:
Number of involved organizations:
Number of attacked organizations:

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

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

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**

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 distributed by the Alert Function

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

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

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 fuction isn‘t available
  - Or outside business hours / during weekends
  - Last resort if no other communication means are available

Participation

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

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

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

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?

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
  - Level of confidence must be given

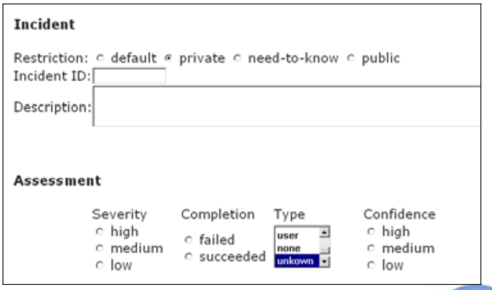
Information Exchange Issues - 3

- **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. :)

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.

The Alert Form



Incident

Restriction: ○ default ● private ○ need-to-know ○ public

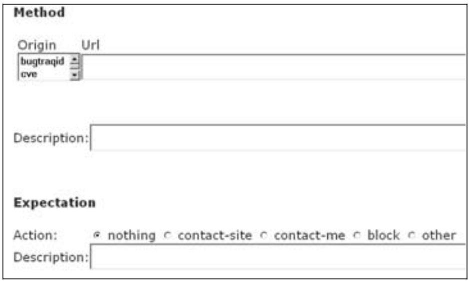
Incident ID:

Description:

Assessment

Severity	Completion	Type	Confidence
○ high	○ failed	user	○ high
○ medium	○ succeeded	none	○ medium
○ low		unkown	○ low

The Alert Form – 2



Method

Origin Url

bugtraqid
cve

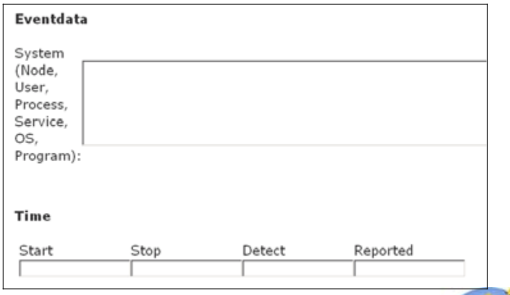
Description:

Expectation

Action: ● nothing ○ contact-site ○ contact-me ○ block ○ other

Description:

The Alert Form – 3



Eventdata

System (Node, User, Process, Service, OS, Program):

Time

Start	Stop	Detect	Reported

In-Band (Internet based) Alert Function

- **Mailing List and Security Gateway**
  - Linux based system
  - Commercial anti-virus software (2 products)
  - 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

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

Outlook for the Alert Function

- **Further out-of-the-Internet services:**
  - Support of SMS
  - Automatic FAX distribution 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

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

---

Thank
you!

Kontakt

Dr. Klaus-Peter Kossakowski

Email: kpk@pre-secure.de
Mobil: (+49) 0171 / 5767010

WWW: https://www.eCSIRT.net

The European CSIRT Network

Code of Conduct

Preamble

Todays networked systems and communications are fundamental for the working of industry, economy, research, administration and government. Networks, systems as well as their applications are complex, disruptable and the target of intentional attacks is a growing threat. There is a need for co-operation between European Computer Security Incident Response Teams (CSIRTs) to

- Improve the security posture of the European Information Technology (IT) infrastructure
- Enable an appropriate and timely response by CSIRTs, to attacks upon the European IT infrastructure
- Raise the awareness by documenting the work of CSIRTs and providing statistical data about attacks and incidents

These are the aspired goals of the partners of the eCSIRT.net project in recognition of their responsibilities:

- CSIC/IRIS-CERT (E)
- DFN-CERT (D)
- GARR-CERT (I)
- Stelvio b.v. (NL)
- NASK/CERT-Polska (PL)
- PRESECURE Consulting GmbH (D)
- RENATER/Le CERT Renater (F)
- UKERNA/JANET-CERT (UK)
- UNI-C/DK-CERT (DK)

Vision

From now on the participiants of the eCSIRT.net project will co-operate in the field of incident handling and build a new community. The take-up of techniques that are proposed within the project will enable the establishment of new best practices and serve the following goals:

1. to enable a standardised and unambigous exchange of incident related information between the CSIRTs involved;
2. to enable the collection of standardised and unambigous incident statistics serving CSIRTs involved and in a generalised fashion, the public;
3. to enable the collection of standardised and unambigous incident related data. This will be followed by intelligent generation of warnings and emergency alerts serving the CSIRTs involved.

Guidelines

The co-operation is determined by the following guidelines:

- The co-operation is voluntary and can be terminated at any time.
- Co-operation within the project will not infringe on partners business.
- Information and intellectual property rights of all partners must be protected.
- The confidentiality of constituent data will be given highest priority.
- Services provided by the partners should steadily improve.
- Policies, procedures and workflows of all partners should be optimized by the exchange of knowledge and practice within the partner community.
- 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.

The eCSIRT.net initiative is open for participation by all European teams that have been shown to follow established best practices by joining the TI accreditation framework (http://www.trusted-introducer.org). Teams outside Europe are welcome to liaise with eCSIRT.net and participate in discussions to progress the goals described above, so they can be implemented internationally. This will also progress the methods and practices developed so they can be utilized and applied in other settings.

Amersfoort, 9 December 2002

CSIC/IRIS-CERT (E)	DFN-CERT (D)
GARR-CERT (I)	NASK/CERT-Polska (PL)
PRESECURE Consulting GmbH (D)	RENATER/Le CERT Renater (F)
Stelvio b.v. (NL)	UKERNA/JANET-CERT (UK)
UNI-C/DK-CERT (DK)	CERT-NL (NL)