



Information Society
Technologies

Report on First Training Workshop

IST-2001-39118

Training of Network Security Incident Teams Staff

TRANSITS



Deliverable no. D2

Project Manager: Karel Vietsch

TERENA, Singel 468 D, 1017 AW Amsterdam, The Netherlands

Phone : +31 20 5304488
Fax: +31 20 5304499
Email: vietsch@terena.nl

Date: 19 November 2002

CONTENTS

Executive Summary	3
1. Workshop Objectives and Background	3
2. Workshop Preparations	3
2.1. Selection of Venue	4
2.2. Choice of Presenters	4
2.3. Workshop Announcements and Selection of Participants	5
2.4. Financial Arrangements	6
2.5. Workshop Materials	6
3. Workshop Delivery	7
3.1. Participants	7
3.2. Programme	8
3.3. Experiences of Presenters and Trainees	9
3.4. Results from Feedback Forms	10
4. Actions Arising	11

Annex I

First TRANSITS Training Workshop materials

Executive Summary

The first TRANSITS training workshop was held in the Oud-Poelgeest Conference Hotel, Oegstgeest, the Netherlands on October 31st and November 1st, 2002. The workshop was judged a great success by both trainees and presenters with everyone contributing to a very useful exchange of information. The trainees asked that a mailing list for the group be established to help them communicate in future, and many indicated that they would be recommending that their colleagues attend future workshops.

1. Workshop Objectives and Background

Increasing the proportion of European networks that have Computer Security Incident Response Team (CSIRT) services is a major part of improving the dependability of networks and promoting public confidence in the Internet. The objective of the TRANSITS project is to promote the creation of more, professional CSIRTs and the strengthening of existing CSIRTs.

Operating a CSIRT takes rare and specialist skills; currently there are only a few hundred experts in Europe who have the necessary knowledge and experience. The TRANSITS project addresses this problem by providing specialist training to staff members of new CSIRTs and new staff members of existing CSIRTs.

Before the start of the TRANSITS project, course materials had already been prepared, but these need to be edited, maintained and updated during the lifetime of the project. A try-out presentation of the course was made in January 2002 in a workshop hosted by Telia at its headquarters in Farsta near Stockholm, Sweden. After the start of the TRANSITS project in July 2002, the earlier material and the feedback from the try-out presentation of the course were taken as inputs for preparing the first edition of the course material. That work was completed in September 2002, and the result was submitted to the European Commission as TRANSITS deliverable no. D1.

During the lifetime of the TRANSITS project the course materials will be presented six times, and it is intended to spread the locations of these six training workshops over various regions in Europe. This document reports on the preparations for, and the delivery of the first of these training workshops.

2. Workshop Preparations

The training workshop required considerable preparations. The two TRANSITS project partners, TERENA (the Trans-European Research and Education Networking Association) and UKERNA (the United Kingdom Education and Research Networking Association), were both involved in this. TERENA's Raquel Corredoira and Karel Vietsch took responsibility for identifying a suitable location, arranging accommodation and arranging financial support to trainees if needed. UKERNA's Andrew Cormack took charge of ensuring the availability of teachers and preparing the contents of the workshop materials. The course was advertised jointly by both organisations, and Andrew Cormack and Karel Vietsch together took

responsibility for the selection of trainees, asking for the advice of prominent members of TERENA's task force TF-CSIRT when needed. TERENA staff produced the printed workshop materials, and TERENA's Dick Visser installed Internet connectivity at the workshop venue.

2.1. Selection of Venue

In view of the intention to spread the locations of the six TRANSITS training workshops over various regions in Europe, it was decided to organise the first workshop in Western Europe, with the second workshop (spring 2003) to be held in Central/Eastern Europe and the third workshop (autumn 2003) possibly in Southern Europe.

Criteria for the selection of the venue included:

- A location at less than one-hour travel distance from a major international airport. Many of the workshop participants have busy diaries and it was felt to be important to keep travel time as limited as possible.
- A secluded venue with the necessary meeting rooms, hotel rooms and facilities for meals in one location. Since the training benefits strongly from personal interactions, also outside the formal sessions, it is important to make intensive use of the 48 hours that trainees and lecturers are together, and encourage them to build up trust relations.
- Moderately priced accommodation. Whilst room hire, meals for workshop participants and travel and subsistence costs of the teachers are paid by the TRANSITS project, trainees are expected to cover their own travel and hotel costs. Some of their employers are not-for-profit organisations with limited means.

After considering several options it was decided to hold the workshop at Oud-Poelgeest castle in Oegstgeest near Leiden, the Netherlands, about 30 kilometres from Amsterdam Airport. TERENA took care of the arrangements with *Congreshotel Oud-Poelgeest*.

2.2. Choice of Presenters

Lecturers were recruited from the most experienced staff members and former staff members of major professional CSIRTs. A number of members of task force TF-CSIRT had committed themselves to contribute to the TRANSITS materials and to act as teachers of course modules at a number of the training workshops. Some of the available volunteers had been co-authors of the original training course materials and/or had presented at the try-out workshop in January 2002.

It was therefore not difficult to find a sufficient number of very well qualified presenters. The following team was chosen:

Andrew Cormack	UKERNA	United Kingdom
Klaus Möller	DFN-CERT	Germany
Gareth Price	BT Ignite Secure Business Services	United Kingdom
Jacques Schuurman	CERT-NL	Netherlands
Don Stikvoort	Stelvio BV	Netherlands

2.3. Workshop Announcements and Selection of Participants

On August 2nd, 2002 the announcement of the training workshop was published on the TRANSITS website (www.ist-transits.org). This announcement contained a course summary, an explanation of the pre-requisites, information about the time and venue and the costs, and instructions on how to apply for participation. At the same time the announcement was sent via the appropriate mailings lists to the members of TF-CSIRT, the FIRST membership and the research and education networking organisations in Europe (the TERENA membership). A reminder was sent to the same communities early September.

Although through this wide distribution the announcement has reached a very large part of the target community, the comment was received later that an even wider audience could have been targeted, for example by approaching all CSIRTs in Europe that are listed by the Trusted Introducer (see www.ti.terena.nl) and/or by spreading the information in the RIPE community (see www.ripe.net/ripe/about/index.html). These suggestions will be taken up in the preparations for the next TRANSITS training workshops.

The following time schedule was mentioned in the workshop announcements:

23 September 2002	Deadline for sending in applications
4 October 2002	Applicants will be notified whether a place has been reserved for them at the workshop
18 October 2002	Deadline for payment of the accommodation costs and the registration fee. In case payment would not have been received before this date, the place at the workshop might be assigned to another applicant.

By the time of the deadline, 25 applications had been received. (Two more applications were received too late.) Because the workshop was planned to accommodate two groups of ten trainees, not all applications could be accepted. Assuming that perhaps not all accepted candidates would be able to participate in the end, it was decided to accept 21 applications.

It was rewarding to see that all applications were of high quality: all applicants satisfied the pre-requisites for participation in the course and all were employed by organisations that either were providing a CSIRT service or had serious and advanced plans to set up such a service. Therefore none of the applications could be dismissed on grounds of quality or relevance.

Still the selection was relatively easy: three organisations/companies that had proposed several staff members for participation in the workshop would be well served by spreading the participation of their staff over this workshop and the next ones, and in one case the organisation concerned would be better prepared for the creation of their new CSIRT at the time of the next workshop. All applicants who could not be assigned a place at the first training workshop were guaranteed a place at the spring 2003 workshop in case they would apply again then.

In the end all 21 accepted candidates confirmed their participation and met the requirement of timely payment of accommodation costs and registration fee. Fortunately it turned out to be possible to accommodate the one extra participant in addition to the originally planned number of twenty.

2.4. Financial Arrangements

As described in the TRANSITS project workplan, all trainees were expected to pay their own accommodation costs at the *Oud-Poelgeest Congreshotel* as well as a (symbolic) fee of 100 euro. Participants were asked to pay these sums to TERENA no later than twelve days before the event. This arrangement not only simplified financial administration, but it also reduced the risk of no-shows.

All participants paid their accommodation costs and fee on time, but the time schedule was obviously rather tight. For future workshops it may therefore be better to allow slightly more time between the notification of acceptance of application and the deadline for payment.

Within the TRANSITS budget, TERENA manages funds to cover part of the travel and subsistence costs of training workshop participants from economically less-developed countries in Europe. This financial support will always cover only part of the total costs of these participants and will be limited to trainees from non-commercial, non-profit organisations. In the workshop announcements it was mentioned that such partial reimbursements of costs could be made available to participants from countries that are qualified by the World Bank as low-income economies (Armenia, Azerbaijan, Georgia, Moldova, Ukraine), lower-middle-income economies (Albania, Belarus, Bosnia-Herzegovina, Bulgaria, FYRoMacedonia, Romania, Russian Federation, Turkey, FR Yugoslavia) or upper-middle-income economies (Croatia, Czech Republic, Estonia, Hungary, Latvia, Lithuania, Malta, Poland, Slovakia).

Only one of the participants in the first TRANSITS workshop applied for reimbursement of part of his costs from these funds. Participation in the workshop from economically less-developed countries was rather limited. This could be caused by the fact that it had been announced that the next workshop will be held in Warsaw, Poland, a location that is more convenient for potential participants from a large number of the countries listed above.

Within the TRANSITS budget, UKERNA manages funds to cover the travel and subsistence expenses of the lecturers who are not UKERNA or TERENA employees. These costs will be reimbursed after the event on the basis of invoices sent by the presenters to UKERNA.

2.5. Workshop Materials

The course was presented using the latest version of the TRANSITS materials. Participants received a workshop pack containing printed copies of the slides, exercises and supporting documentation. Digital copies of these materials were provided on the workshop CD-ROM, which also included the CSIRT Handbook (with thanks to the copyright holders, Carnegie Mellon University) as well as RFCs relevant to CSIRT work. Each participant pack also included a copy of the book *Incident Response* by Kenneth R. van Wyk and Richard Forno

(published by O'Reilly & Associates, Inc.) and a Guidance Note on writing advisories published by UKERNA.

As the course materials cover rapidly developing topic areas and benefit continuously from feedback, some slides were modified immediately before and even during the workshop. These will be e-mailed to participants in due course.

3. Workshop Delivery

3.1. Participants

Twenty-one trainees attended the course, from fourteen countries:

Cathy Booth	UNIRAS	United Kingdom
Mercedes Cantos	European Space Agency	Netherlands
Micael Carlsson	Telia	Sweden
Tim Charrot	QinetQ	United Kingdom
Maria Dahl	SINTEF	Norway
Eftychios Eftychiou	University of Cyprus	Cyprus
Pierre Forget	CERT-IST	France
Manuel Garcia	esCERT	Spain
Erik de Jong	CERT-RO	Netherlands
Ulrich Kiermayr	ACOnet	Austria
Stelios Maistros	GRNET-CERT	Greece
Gilles Massen	RESTENA	Luxembourg
Janos Mohacsi	HUNGARNET	Hungary
Peter van Os	CERT-KUN	Netherlands
Lillian Røstad	SINTEF	Norway
Jürgen Sander	PRESECURE	Germany
Michael Schmidt	Deutsche Telekom	Germany
Rune Sydskjør	UNINETT-CERT	Norway
Vincent Thiele	CERT-RO	Netherlands
Debora Tonelli	European Space Agency	Italy
Marius Urkis	LITNET-CERT	Lithuania

The organisers were particularly pleased to welcome participants from three EU Accession States: Cyprus, Hungary and Lithuania. Of the trainees, fifteen work for existing CSIRTs and six were from organisations in the process of creating a new CSIRT. Four of these organisations had not participated in European CSIRT activities before. The participants represent all sectors of the European Internet: five from commercial companies, eleven from research and education networks and organisations, and five from government organisations. With the presenters also having experience of all sectors, this gave good opportunities to share knowledge both within and across sectors.

3.2. Programme

The objectives of the training workshop were:

- to understand where CSIRTs fit into the organisation
- to understand the tasks and tools that are necessary to perform their function
- to develop and practice the skills that are needed by a CSIRT team member
- to understand the external issues (both legal and technical) that may effect the operation of a CSIRT.

The course consisted of five modules. Some of these included exercises that the trainees had to complete and discuss, while others included time for discussion among the whole class. The modules were:

- **CSIRT Organisation**

Describes how CSIRTs fit into their organisations; planning the CSIRT, defining the constituency of the team and gaining management authority for it, deciding the services the team will offer, working with those outside the organisation, staffing the CSIRT, funding. Trainees discussed their own organisation and how their team fits into it.

- **Technical Aspects**

Understanding how intruders attack systems; intruders and their motivations, network protocols and how they can be abused, operating systems and services, types of vulnerability, information gathering, breaking in, hiding traces, denial-of-service attacks. A number of exercises were used to show how these appear in practice.

- **CSIRT Operations**

Describes the facilities, systems and tools needed by CSIRTs to operate successfully; housing the CSIRT, equipment, e-mail, remote access, information and contacts, servers and networks, incident response plans and procedures, tracking systems. As an exercise trainees discussed and developed incident response plans for their own teams.

- **Legal Issues**

Looks at the areas of legislation that are likely to affect CSIRTs in their work and that team members need to be aware of; origins of computer legislation, problems, data protection, computer misuse, working with law enforcement, monitoring, evidence, European developments.

- **Working with Vulnerabilities**

Discusses the roles that CSIRTs may decide to play in distributing and producing information about vulnerabilities; why do vulnerabilities exist, what should CSIRTs aim to do, sources of information and how to use them, advisories – distribution, interpretation, investigation and co-ordination.

The modules were presented in parallel in two groups. In order to encourage interaction with participants not known to them earlier, trainees were divided over these groups such that people from the same organisation were not in the same group and the number of participants with the same mother language in each group was minimised.

The time schedule of the two workshop days was as follows:

Thursday October 31st

Time	Group 1 in “Wapenzaal” room	Group 2 in “Willinkkamer” room
09.30	Welcome and introductions in “Wapenzaal” room	
10.00	Organisational Issues	Operational Issues
12.30	Buffet Lunch	
13.30	Organisational Issues (report back)	Operational Issues (report back)
14.30	Legal Issues	Technical Issues
16.30	Vulnerabilities	Technical Issues (cont.)
18.00	Close	
19.30	Dinner	

Friday November 1st

Time	Group 1 in “Wapenzaal” room	Group 2 in “Willinkkamer” room
09.00	Operational Issues	Organisational Issues
12.30	Lunch	
13.30	Technical Issues	Vulnerabilities
15.30	Technical Issues (cont.)	Legal Issues
17.00	Close	

Group 1: Cantos, Charrot, Dahl, Kiermayr, Maistros, Massen, Mohacsi, Schmidt, Sydskjør, Thiele, Urkis

Group 2: Booth, Carlsson, Eftychiou, Forget, Garcia, De Jong, Van Os, Røstad, Sander, Tonelli

3.3. Experiences of Presenters and Trainees

The workshop was judged a great success by both presenters and trainees with everyone contributing to a very useful exchange of information. The participants asked that a mailing list for the group be established to help them to communicate in future, and many indicated that they would be recommending that their colleagues attend future workshops.

The venue contributed significantly to the success of the workshop. The training area contained two teaching rooms, allowing the participants to meet all together or split into smaller groups. The formal sessions were presented to groups of ten and eleven trainees, with two tutors attending each session. A social area between the training rooms allowed for informal discussions and work in smaller groups. Accommodation and dining areas were also on the same site, within walking distance, which gave the maximum opportunity for exchange of information and the development of trust relations. A wireless network was installed in the training area by TERENA: this allowed tutors and trainees to consult websites for up-to-date information and was considered a useful facility.

Every trainee was asked to fill in a feedback form during the course to rate the content and presentation of each of the modules, and the workshop organisation and venue. Written comments were also sought to help in developing the materials and organising future workshops. Marks were requested for each module for level and quantity (from 1, trivial, to 5,

excessive), for usefulness, organisation, visuals and delivery (from 1, low, to 5, high). Marks on the latter scale were also requested for workshop announcements, application and selection process, pre-workshop information, meeting rooms, Internet connectivity, hotel rooms, meals and support staff. Twenty completed feedback forms were received. Overall the results were very positive, with the modules averaging between 3.0 and 3.6 for level and quantity, 3.2 to 3.8 for usefulness, and 3.8 to 4.1 for the presentation aspects. Logistics scored between 4.0 and 4.4 and the venue between 3.5 and 4.2.

The technical module seemed to both attract people and overwhelm them: it had the highest score for level, quantity and usefulness, and had written comments requesting even more!

The written general comments were also very positive: “very positive experience”, “great course”, “great workshop” and “good material that a starting team needs to establish itself and very helpful guidelines for established teams to improve their effectiveness” indicate that the workshop achieved its objectives. Details of the feedback scores are given in the next section.

3.4. Results from Feedback Forms

Mean scores were as follows (all scores on a range from 1 to 5 – see section 3.3 for details):

Module:	Organisation	Legal	Vulnerabilities	Operational	Technical
Level	3.05	3.15	3.05	3.13	3.60
Quantity	3.25	3.15	3.00	3.30	3.55
Usefulness	3.21	3.35	3.45	3.60	3.75
Organisation	4.05	4.00	3.95	4.00	4.05
Visuals	3.80	3.85	3.75	4.00	4.00
Delivery	4.15	4.00	3.95	4.10	4.00

Logistics	
Announcements	3.95
Application & Selection	4.00
Pre-workshop information	4.22
Meeting rooms	4.16
Internet connectivity	3.79
Hotel rooms	3.47
Meals	4.21
Support staff	4.39

4. Actions Arising

The following action items will be taken up in the TRANSITS project as a result of the experiences from the first training workshop:

- The course modules will all be revised in the light of comments from trainees and presenters during the course. Planned changes range from changes to some phrases on slides that were not clear to an audience whose first language was not English, to the addition of new sections to the organisation and vulnerabilities modules.
- A mailing list will be created for the participants from the course to enable discussions to continue. Updated versions of the course materials will be distributed to the delegates through this list.
- The successful aspects of this venue will be considered in the choice of venue for future workshops.