Developments in the area of Security as reported in The Works of DANTE

DECEMBER 1996 - DANTE/UKERNA PARTNERSHIP TO SET UP SIRCE SERVICE

The TERENA Executive Committee has announced its intention to award the set-up of a pilot European Security Incident Response Coordination Service to a partnership consisting of DANTE and UKERNA. UKERNA is the UK organisation responsible for the operation and development of JANET and SuperJANET.

The establishment of a European Security Incident Response Coordination Service was discussed and requested by the European IRTs (Incident Response Teams) to solve a number of coordination problems. These include dependence of European IRTs on the US funded CERT/CC, as well as those arising from cultural, legal and language differences, and different time zones.

In consultation with its CERT Task Force, the TERENA Executive Committee set up a Technical Advisory Group (TAG) to advise TERENA on a suitable organization to lead a two and a half year pilot service. At the beginning of October 1996, TERENA issued a call for proposals to a limited number of organisations for the operation of the SIRCE (Security Incident Response Coordination for Europe) pilot.

DANTE and UKERNA decided to respond to the call by establishing a partnership which brings together the complementary skills of the two organisations. UKERNA has the technical expertise of the well- established JANET-CERT, while DANTE has the commercial and administrative experience in the management of coordinated pan- European services.

The pilot service is planned to be launched in the first quarter of 1997. DANTE and UKERNA, in consultation with TERENA, will immediately start preparing the service implementation, one element of which is the drafting of a detailed service specification.

As required in the specification of the TERENA CERT Task Force the service will develop gradually. In the initial phase a coordination function will be offered, which includes organisation of meetings, help for the establishment of new IRTs, and the provision of information services. In the second phase of the pilot incident coordination will be included, and SIRCE will be involved in the process of responding to individual incidents. After the pilot phase it is intended that an operational service will provide full incident coordination, 24 hours/7 days a week.

AUGUST 1997 - EUROCERT TAKING SHAPE

The contract for the provision of a European Incident Response Coordination service between TERENA and the DANTE/UKERNA partnership has been in effect for over 3 months. The service is delivered under the name EuroCERT. Initially EuroCERT consists of an information resource, primarily targeting European Incident Response Teams (IRTs). This includes a point of contact available during normal office hours. Work on the Web site (http://www.eurocert.net/) has progressed and most of the basic information and facilities described in the contract (including an FTP server and mailing lists) are now available.

EuroCERT aims to cover all European IRTs. Therefore we are in the process of collecting the up-to-date contact information of all European IRTs. Currently we have details of 22 IRTs. We are still seeking information from another 15 that we know about while there may be others of which we are as yet unaware. The list of the European IRTs known to EuroCERT can be found here: http://www.eurocert.net/euro-irts.html. A template is available for IRTs to provide EuroCERT with contact information: http://www.eurocert.net/cert-blank.html.

During the next few months the EuroCERT team will be concentrating on producing a revised proposal to TERENA for a Basic Incident Coordination service for European IRTs. In this next

stage of the pilot EuroCERT will become actively involved in coordinating security incidents that effect more than one Incident Response Team.

OCTOBER 1997 - EUROCERT PLAN FOR INCIDENT COORDINATION

EuroCERT, the European Incident Response Coordination Service, operated under a contract between TERENA and the DANTE/UKERNA partnership has been in operation for 6 months and is now producing plans to move to a live incident coordination service. The EuroCERT team is preparing a specification which when finalised will be used to move the service from being primarily an information resource to actively providing security incident coordination for European Incident Response Teams (IRTs).

Currently nine organisations are contributing financially to the pilot: ARNES (Slovenia), CNUCE (Italy), DFN (Germany), NORDUnet (Nordic countries), RedIRIS (Spain), SURFnet (Netherlands), SWITCH (Switzerland), UKERNA (United Kingdom) and UNINETT (Norway). ACONET (Austria) will join imminently with several others expected soon. Contributors will receive a priority service when incident coordination commences. EuroCERT will move to a more complete incident coordination service as more contributors become involved. EuroCERT is holding an open meeting co-located with the FIRST (Forum of Incident Response and Security Teams) technical colloquium in Milano, Italy on 12 January 1998. This meeting is primarily aimed at European IRTs, but is open to all. The agenda will include presentations by EuroCERT, discussions and presentations on Incident response and a PGP signing party.

FEBRUARY 1998 - EUROCERT INCIDENT COORDINATION SERVICE NEARS ACCEPTANCE

EuroCERT, the European Incident Response Coordination Service, operated under a contract between TERENA and the DANTE/UKERNA partnership has been in operation for 10 months of the original 12 months contract. In January 1998 UKERNA presented a proposal to TERENA for an Incident Coordination service to start in May 1998. This proposal was accepted in principle and they are currently in the process of finalising the details of the contract with TERENA. DANTE will still retain a presence in the project after the completion of the initial contract period at the end of April 1998, with the prospect of more active involvement at a later stage.

Currently the following eleven organisations are contributing to EuroCERT: ACONET (Austria), ARNES (Slovenia), CNUCE (Italy), DFN (Germany), NORDUnet (Nordic countries), RedIRIS (Spain), Renater (France), SURFnet (Netherlands), SWITCH (Switzerland), UKERNA (United Kingdom) and UNINETT (Norway). EuroCERT held an open meeting co-located with the FIRST (Forum of Incident Response and Security Teams) technical colloquium in Milan, Italy on 12 January 1998. This meeting was very successful with thirty-six people attending from locations around Europe and North America. The occasion was used as an opportunity for IRTs to share information and to discuss how EuroCERT should move forward towards Incident Coordination. The minutes and copies of the presentations are available from the EuroCERT web site http://www.eurocert.net .

JUNE 1998 - DANCERT

DANCERT is the Computer Emergency Response Team (CERT) pilot project serving DANTE customers. DANCERT is planned to be a security response facility relating to attacks on DANTE operated services, including the TEN-34 network. It deals with computer and network security incidents related to hacking and infrastructure vulnerabilities that involve services operated by DANTE. In addition DANCERT deals with large scale Spam attacks involving the networks operated by DANTE.

The main aims of DANCERT are to provide DANTE customers with the coordination for the handling of network security incidents, the distribution of security information to help prevent

security incidents and with a focal point for security related activities involving the DANTE services.

JAN/FEB 2001 - SECURITY

The design and implementation of a new tool was completed. This tool, based on flow monitoring, is aimed at detecting Denial of Service (DoS) attacks when they occur. It has shown that TEN-155 is almost constantly carrying such attacks, and many DANCERT trouble tickets have been raised to tackle this. However, tracing such attacks to the source has proven difficult, and a faster inter-domain co-operation between CERTs will be required in the future. Development of this tool continues in order to eventually produce statistics.