Security Incident Coordination at the RIPE NCC ?!

Daniel Karrenberg

Document: ripe-149
Date: October 30th 1996

Scope

This document describes why the RIPE NCC should provide security incident coordination for the European Internet service providers. It presents the position of the RIPE NCC. Discussion and comments to the author are very welcome.

Summary

A TERENA pilot project for security incident coordination is due to start in Q1/1997. After reviewing the description of the pilot service we concluded that the NCC should provide this service because this is in the interest of the European ISPs. The RIPE NCC will submit and publish a proposal to execute the pilot. We call on the ISPs to support this and to commit financial contributions in order to firmly establish their interest in such a service and to help make it a success.

Background

The need for security incident coordination in Europe has been undisputed for quite some time. Yet no initiative to set up such a service has gathered sufficient momentum to come to fruition. After thorough preparatory work by its CERT task force TERENA has recently issued a closed call for proposals for a pilot service dubbed SIRCE (Security Incident Response Coordination in Europe). The RIPE NCC is one of the recipients of this call. At their annual meeting the RIPE NCC contributors committee authorised the RIPE NCC to respond to such a call if the service was beneficial to the contributors and this activity was funded separately from NCC core activities.

The SIRCE Pilot Project

The service described in the call for proposals explicitly excludes the handling of incidents itself. SIRCE is strictly limited to *basic incident coordination*. The actual handling of incidents is done by incident response teams (IRTs) operated by ISPs and others. Incident coordination includes the setting up of contacts and trusted information channels between IRTs, tracking who is working on a particular incident and keeping the IRTs involved informed about progress. In addition to incident coordination itself, SIRCE will provide support functions for IRTs such as helping new IRTs to start up, organising meetings and publishing general information about incident response.

For details about the services see the task force report at `ftp://ftp.ripe.net/ripe/misc/cert-eu.ps` and the RIPE NCC proposal (to be published).

The two things that remain unclear about the pilot project are the funding and the way the project is going to be managed by TERENA. TERENA expects to obtain funding but does not give any particulars. Also the changeover from the pilot to a regular service is not addressed at present.

Time Schedule

The call for proposals was received at the NCC on October 4th. Proposals are due by November 1st. Interviews with short-listed candidates are scheduled for the beginning of December and TERENA expects to decide on the execution of the pilot by December 31st. The pilot is due to start Q1/1997.

The Internet Service Providers

After considering the description of the pilot service we believe that the ISPs have an interest to see this pilot executed at the RIPE NCC. ISPs are currently handling incidents within their own infrastructure and possibly customer infrastructures as well. Whether an ISP currently has an IRT as such does not really matter as we expect them to have at least informal structures to deal with security incidents. We observe that there is a general interest in coordination but no focus as yet. The project will provide such a focus. We also expect that ISPs have an interest in coordination focussed on their needs rather than those of others such as software/hardware vendors, governments, news media and law enforcement agencies. In case of conflicts the RIPE NCC will clearly choose to defend the interests of the ISPs. In addition ISPs also have an interest to have this sensitive function executed by an organisation that is neutral and impartial vis a vis the interests of different ISPs involved.

The RIPE NCC

The NCC is ideally suited for providing this service for a number of reasons:

- we are already serving the ISPs who are the main target group,
- we already have relationships of trust with ISPs,
- we already have years of coordination experience on the scale required including the knowledge and the tools to make it work,
- we are already accepted as being neutral and impartial vis a vis different ISPs,
- we already maintain the RIPE database which is very frequently used to find contacts for incident coordination,
- we have a solid track record of piloting services and turning them into stable and reliable operational services.

Funding

We believe that finding the funding of the pilot project should not be left totally to TERENA but rather that as many ISPs as possible should contribute from the outset. The main reason is to clearly establish that a real interest exists in the ISP community. Secondary reasons are to establish influence by the target community as early as possible and to facilitate transition to a normal service.

We also believe that the level of resources for the pilot envisioned by TERENA is too low to guarantee a successful service for the size of community we expect. So additional funds will be needed.

The NCC has a proven mechanism of running pilot projects funded by interested parties, which can quickly be turned into regular services. Exactly when this would happen and whether the SIRCE service will be either a core service funded by all NCC contributors or an additional service funded only by a subset of contributors is to be decided later on. TERENA aims for a pilot taking "no longer than 2.5 years". We will aim for an operational service by Q1/1998.

The expected benefits for those funding the pilot are:

- preferred service and support, non-contributors will receive service on a time-permitting basis when there are no requests from contributors;

- direct channels such as private mailing list for contributors to discuss directions and influence pilot;

- public credit for their contribution.

In the unlikely case that there will be no significant funding commitments from the ISP community, we will have to conclude that interest is not sufficient and the RIPE NCC will have to withdraw its proposal.

TERENA Involvement

We believe that TERENA should be involved in managing the pilot project because its CERT task force has outstanding expertise and they have spent significant resources to define SIRCE services in a way that is right and very useful for ISPs. They also have significant support from existing IRTs.

With the pilot being executed at the NCC and the ISPs contributing to the funding everyone wins; TERENA wins by getting credit for taking the lead and managing the pilot, the ISPs win by getting a service responsive to their needs and interests earlier than without TERENA's initiative. There will generally be low entropy.

The situation is somewhat awkward as the NCC currently is formally part of TERENA. This can be overcome since NCC is managed very independently and the principle of formal separation of the NCC from TERENA by Q1/1998 has already been agreed by all involved parties. TERENA has also taken care that proposal review process is fully independent and neutral.

Further Actions

Time for further actions is short because of the tight time schedule.

The NCC will respond to the call for proposals by November 1st. The proposal will include the policies described above, propose ISP funding to TERENA and request discussions about project management. It will state that we have called for support from our community including financial contributions. It will reserve to withdraw at the interview stage if support should be insufficient at that time.

We will publish our proposal on November 4th including a call for support and funding commitments for the pilot.

ISPs should react to the call for funding commitments as quickly as possible but before November 27th.

We will keep the community informed about further developments.