Security Incident Response Coordination in Europe

Pilot Project Proposal

Daniel Karrenberg
Carol Orange
Paul Ridley

Document: ripe-150
Date: November 5th 1996

Scope

In this document, we propose to execute a pilot project for Security Incident Response Coordination in Europe (SIRCE) at the RIPE NCC. We present relevant information about the RIPE NCC, including the reasons why the NCC offers a uniquely suitable setting for the SIRCE project.

1. Background

The need for security incident coordination in Europe has been undisputed for quite some time. Still, no initiative to start 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 was one of the recipients of this call. At its annual meeting, the RIPE NCC contributors committee requested that the NCC consider the call for proposals with respect to its usefulness for the European ISPs, and if deemed beneficial, that the NCC respond to such a call. It was also agreed that this activity should be funded separately from NCC core activities. Having considered both the call for proposals, and the final report on "CERTs in Europe" prepared by the TERENA Task Force (`ftp://ftp.ripe.net/ripe/misc/cert-eu.ps`), we propose that the SIRCE pilot project be performed at the RIPE NCC.

2. The RIPE NCC

Before delving into the project itself, we first give a brief sketch of the RIPE NCC, the context within which this project would be performed.

The mission of the RIPE NCC is to coordinate Internet operations in Europe and surrounding areas. In this section, we give an overview of the activities, customers, organisation and funding of the RIPE NCC. Those familiar with the NCC may want to skip ahead to the next section.

2.1. Principles for RIPE NCC Activities

The RIPE NCC performs activities for the benefit of the Internet service providers (ISPs) in Europe and the surrounding areas, primarily activities that the ISPs need as a group, although they may be competing with each other in other areas.

The RIPE NCC observes strict neutrality and impartiality with respect to individual service providers. In particular, activities which are clearly in the domain of the ISPs themselves are not performed at the NCC.

Activities are defined, performed, discussed and evaluated in an open manner. Results of activities such as software tools are made available to the public. All budgets and actual income and expenditure reports are published. Individual data is kept in confidence as required. For example, the amount of address space allocated and assigned to an ISP is published as are database entries of the individual assignments including relevant contact details. Sensitive information submitted to support an individual assignment request, on the other hand, is kept in strict confidence.

Whereas performing a specific activity may result in services being provided to one or more ISPs, the result must benefit the European ISPs as a whole. Address space registration services, for example, are provided to ISPs individually, but the activity as such benefits all ISPs by distributing address space according to common standards and by maintaining a neutral and accessible registry.

2.2. Activity Areas

RIPE NCC activities can be grouped into four categories. We briefly describe each category below to give an indication of the context within which we suggest the SIRCE project be performed.

Registration Activities

These activities are related to the NCC's role as the Regional Internet Registry (IR) for Europe and surrounding areas. It includes the evaluation and handling of requests for allocation and assignment of IP address space, the management of reverse domains associated with this address space, and auditing and quality control to ensure fair and expedient processing of requests. Also included in this area are training activities for Local Internet Registries, production of documentation related to Internet registration policies and procedures, and activities which ensure the proper set up of new local IRs.

Services performed in this area are only accessible to formally established local IRs which contribute to the funding of the NCC.

Coordination Activities

The activities grouped in this area are quite diverse. Their common purpose is to support the coherent operation of the Internet in the European area. An important activity is the provision of access to the RIPE database in which information about address space and routing policies together with the appropriate contact points is registered. Developing and publishing the RIPE database software is also part of this area, as is the provision of information services for ISPs and the general public via the Internet. Operational coordination such as efforts to reduce the number of globally visible routing prefixes also fall into this category, as does the production and publication of software tools for such efforts.

In order to be effective, the services performed in this area must to be accessible to the general Internet public. These services are made available via the web (see http://www.ripe.net), and ftp (see ftp://ftp.ripe.net), together with a range of information useful to the European Internet community as a whole. Moreover, progress is reported to the appropriate RIPE working group at RIPE meetings at which point feedback is gained on the priorities, problems and needs of the European ISPs. The RIPE meetings, organised by the NCC 3 times per year (see ftp://www.ripe.net/ripe/Next-Meeting), are open to anyone interested in Internet developments in Europe.

The contributors to the funding of the NCC receive precedence over all others when special support is needed.

Administration Activities

This area covers all regular reports published by the NCC, administrative support for RIPE as well as general administrative overheads which cannot be clearly attributed to a specific activity. As such, it includes production of the Quarterly Reports and the resources needed for charging, billing and the general financial administration.

New Activities

This area represents those activities that are either entirely unforeseen or cannot be fully specified at the time of this writing. The existence of this area gives the NCC the flexibility to react quickly to the rapidly changing needs in today's Internet. Activities in this area are often suggested by the appropriate RIPE working group.

If the activities turn out to need long term support they may become a regular NCC activity funded by all contributors later. If the activities are short term but substantial, or continued support by all contributors is not appropriate, they may be continued as special projects for which funding is sought separately among interested parties. These new activities are executed under the guidance of the RIPE working groups. It is assumed that representatives of the contributors participate actively in these working groups.

The PRIDE project and the creation of the routing registry are good examples of such activities as is the startup of IPv6 coordination.

2.3. Organisation

The RIPE NCC is located in Amsterdam, The Netherlands. It has been operating since April 1992 and currently has more than 450 customers and a staff of 15. By the end of 1997 it is expected to serve more than 900 customers with a staff of 32. The operating expenses for 1997 are budgeted at kECU 1984.

The NCC is currently operated as a service of the TERENA Association but is managed quite independently. It has recently been agreed to bring the NCC activities under a separate legal entity controlled by its customers.

2.4. Funding

The RIPE NCC is fully funded by its customers, the European ISPs. It has a tradition of starting new activities and pilot projects funded by interested parties, and extending them to meet the needs of the European ISP community as required.

2.5. Further Information

More information can be obtained from the RIPE NCC web site at `http://www.ripe.net/`. The RIPE NCC routinely publishes information about its activities in the RIPE document series. The documents are numbered and document *ripe-nnn* can be found alternatively at

`http://www.ripe.net/docs/noframes/ripe-nnn.html`
or
`ftp://ftp.ripe.net/ripe/docs/ripe-nnn.ps` (PostScript)
or
`ftp://ftp.ripe.net/ripe/docs/ripe-nnn.txt` (Ascii)

An index of all RIPE documents is maintained in

`ftp://ftp.ripe.net/ripe/docs/ripe-index`

For details about the activities, customer base and and expenditure, please refer to *RIPE NCC Activities & Expenditure 1997* (ripe-144). For details of charging see *RIPE NCC Charging Scheme 1997* (ripe-146). Recent activities are described in the quarterly reports published in the same series.

Security Incident Coordination at the RIPE NCC ?! (ripe-149) is a position statement which describes why the RIPE NCC should execute this pilot project.

3. The SIRCE Pilot Project at the RIPE NCC

In this section we describe the details of the SIRCE project as we propose to execute it at the RIPE NCC. In particular, we discuss operational policies, services to be provided, the project plan, the financial plan, and open issues.

3.1. SIRCE Policies

The policies established for the pilot project will determine the long term success of SIRCE in enabling the European Internet community to handle security incidents in an effective and timely manner. Should the project be performed at the RIPE NCC, the detailed policies will be determined by the customers. However, we propose the following provide a basis from which to start.

- Customers of the SIRCE pilot project are IRTs, the majority of which are expected to be based in European ISPs.

- The SIRCE pilot project will be customer oriented. Paying customers will receive priority service. Non-paying customers will receive service on a time-available basis if there is no work outstanding for paying customers.

- The SIRCE pilot project will be developed into a fully operational service as early as feasible. This will establish clarity in the European Internet community regarding what can be expected from SIRCE, which in turn will encourage participation in the incident coordination efforts from the start.

- In the pilot phase, we aim to get a significant number of ISPs as paying customers. This will stimulate security mindedness among the European ISPs and ease the handling of incidents affecting European Internet users. It will also make the transition from the pilot into a regular service easier.

- If conflicts of interest between ISPs and other organisations such as software/hardware vendors, governments, news media and law enforcement agencies arise, the interests of the ISPs shall be of primary concern.

- Customer IRTs will be treated in a strictly neutral and impartial fashion.

- Activities which are clearly in the domain of the customers will not be performed by SIRCE.

- All SIRCE project activities will be defined, performed, discussed and evaluated in an open manner.

- Software tools, statistics and other results of SIRCE activities will be made publicly available.

- All budgets, income and expenditure will be published.

- Individual data, especially particulars about incidents handled will be kept in strict confidence.

These policies are consistent with general RIPE NCC policies which have been established in cooperation with the European ISPs, and have proven effective in that context.

3.2. SIRCE Services

The services of the pilot project will be those described for Basic Incident Coordination (BIC) in Section 2.2.1 of the CERTs in Europe Report produced by the TERENA Task Force. This includes the services described for Incident Support in Section 2.1.1 of that document.

Many of the incident support activities will be provided as extensions of current RIPE NCC activities. For example, the information services currently provided by the NCC will be extended to include SIRCE. Regular meetings of SIRCE contributors can easily be held in conjunction with RIPE meetings, held three times per year. We believe holding meetings three times rather than once per year will facilitate customer involvement and feedback which is crucial to th success of the pilot project. The RIPE meetings also provide an excellent opportunity to promote the need for IRTs in Europe, and to pull the ISP community into the effort.

To assist the startup of new IRTs, we plan to extend our current course program to include a course on setting up and operating an IRT. This would be a one day course, organised much like the Local IR courses currently held throughout Europe. This may be complemented by courses on Internet Security in a later phase to help IRTs stay current on developments. All course material will be made publicly available to enable IRTs to educate their customers as well.

The relative priorities and requirements of the different support services will be set according to customer demand. Input from customers will be gained by holding meetings open to all contributing IRTs, and by establishing an advisory group consisting of customers and invited experts.

The key service of the pilot will be incident coordination. Therefore we describe in more detail how we propose to implement it at the RIPE NCC.

The Basic Incident Coordination Service

In the remainder of this section, we provide details on the Incident Coordination service as we propose to implement it at the RIPE NCC. While detailed BIC policies and procedures will need to be established, we envisage BIC to encompass the following service elements:

- When SIRCE is first notified of an incident, it will be logged, and a ticket will be opened to track further messages and information which pertain to it. A ticket number will be assigned, which will be made available to the appropriate parties when referring to the incident. This facilitates further communication and event tracking for the incident.

- We will then work to identify the IRTs, ISP NOCs, and others who should be involved in handling the incident. They will be notified of the incident, its current status, and of the other parties involved.

- As progress is made, we will work together with the IRTs to track who is working on which aspect of the handling of the incident and communicate this to all parties involved.

- We will close the incident when those involved agree that it is either resolved or that there is no more work in progress.

- We will then log a summary of the incident and post it to all involved if appropriate.

- Incidents, while open, and after being closed will be logged in such a way, that a recurrence will be identified. Should an incident be identified as being very similar to a previous one, the relevant incident information will be provided to the parties involved.

4. SIRCE Pilot Project Plan

We plan to have an initial incident coordination capability as soon as possible and much sooner than envisaged in the TERENA task force report. We expect requests for incident coordination to be submitted as soon as SIRCE is announced. We prefer to deal with the initial requests on a best-effort basis rather than explain that we are not yet in that project phase. Not doing so will result in a significant loss of credibility and confusion will arise as to what kind of services will actually be provided by SIRCE.

For the same reasons, regular incident coordination (normal rather than best-effort service) will be provided as early as possible. To achieve this, we plan to ramp up staffing to three FTE as soon as practical but before three months have elapsed rather than to wait for the time suggested in the call for proposals.

4.1. Project Phases

We have divided the pilot project into three logical phases. In this section, we indicate the key activities involved in each phase.

Set Up Phase

Before the initial incident coordination capability can be offered, a number of activities will have to be performed to set things up. This phase is expected to take roughly two months, and definitely not more than three.

The work items to be performed in this phase include:

- Establish local working environment. A suitable computer infrastructure which addresses the projects needs (security, connectivity, work flow software, etc), along with the physical requirements (again including security) will be set up.
- Establish contact with customers, peers and relevant groups. A customer base will be established, and personal trusted contacts built up to be used in incident coordination. Moreover, contacts with experts and established CERTS will be actively pursued.
- Establish contact with project management. The project planning, budgets, and reporting will be worked through together with the project management.
- Hold the first meeting of customers and establish advisory group. Advice will be sought on the priorities and needs in the user community.
- Establish policies and procedures for BIC services in particular, and for SIRCE services in general.

- Hire additional staff. Before the BIC can become operational, experts will be required to coordinate reported incidents.
- Develop and document the initial BIC capabilities.

Initial Coordination Capability

During this phase of the project, we will start basic operations on a best effort basis. As we do so, we will review and refine our procedures in preparation of the regular capability services. Sometime during this stage SIRCE may be announced to a larger audience. Project efforts will include:

- Start BIC on best-effort basis. We will provide the services defined in Section 3.2 to the extent our resources permit.
- Customer contacts will be strengthened and personalised, as will be facilitated by contacts made in providing the initial coordination capabilities.
- The procedures will be reviewed and refined based on the practical experience gained in providing the initial services.
- Other general services defined in the CERTs in Europe report will be extended based on customer needs and priorities.
- Develop the normal coordination capability.

This phase will not last longer than three months.

Regular Coordination Capability

In the final phase of the pilot project, the BIC services will be fully operational, feedback will be sought from customers, and steps will be taken to move the service to an established, fully operational service for Security Incident Response Coordination in Europe. This stage will be reached 6 months after the start of the project. The nature of the activities in this phase will include:

- The BIC services will be fully operational. This means that in addition to the services specified for this phase in the CERTs in Europe report, the incident coordination services specified in Section 3.2 will be applied to all incoming incidents.

- Additional meetings of customers will be held to review the activities and to gain feedback on the services provided.

- Based on the experience gained in the pilot phase, and on the customer feedback, the infrastructure and services will be extended to establish the SIRCE services for the long term.

4.2. Implementation Details

The remainder of this section will describe some details of how we plan to implement SIRCE addressing questions raised in the call for proposals.

Personnel

The project will be directed by Daniel Karrenberg, the general manager of the RIPE NCC. He has considerable experience in setting up and running coordination services as well as in network/computer system operations and security. Once the decision to start the pilot is made we expect to hire a full time SIRCE manager very quickly. Her first task will be to start the set-up phase activities and to hire additional staff. We are in contact with suitable and competent candidates already. Given the sensitivity of the project, we may not hold an open hiring process for the initial staff. We plan instead to approach selected individuals based on recommendations from existing IRTs and customers. In the initial stages and later on in case of emergencies SIRCE will be able to draw on existing RIPE NCC staff resources if necessary.

Physical Location and Security

The location of SIRCE will be the Amsterdam metropolitan area. The nearest airport is Amsterdam Schiphol, a major European airport. The RIPE NCC is planning to relocate within this area in the first half of 1997. The current location is reachable by taxi from the airport in approximately 20 minutes. The requirements for the new location include good connectivity to pubic transport including to/from the airport.

In both the current and the new location SIRCE staff will be located in separate offices with physical access control and a specific access policy.

The current location has 24 hour security guards, but physical access to the office doors of our offices is not controlled tightly as we share the building with other organisations. The new location will improve this. If possible we will reserve a closed corridor or wing for SIRCE offices.

Computer Infrastructure, Connectivity and Security

The RIPE NCC is currently operating all the systems and software which will be needed by SIRCE. We employ standard security measures such as different security strata for networks and machines, dial back for dial-up access, one time passwords and encrypted sessions for access from the outside, packet filtering on exterior routers and extensive logging of security relevant events. This experience will ensure a quick start of the SIRCE infrastructure.

SIRCE staff workstations and servers will be fully separated from the RIPE NCC infrastructure. Physically separate networks will be installed. SIRCE and the NCC will only share the redundant exterior routers connecting both to the Internet. If necessary SIRCE may use the information services of the RIPE NCC such as HTTP and FTP during the set-up phase. Eventually however these services will be fully separated from the NCC too.

We are connected to the Internet both at the Amsterdam Internet Exchange and with private connections. All connections are at 10Mbit/s. It is RIPE NCC policy to peer with any customer who wishes to do so and provides the connection. We are currently connected to the following autonomous systems:

AS286 - EUnet Backbone AS
AS1103 - SURFnet
AS1104 - NIKHEF-H
AS1128 - EuropaNET
AS1200 - Amsterdam Internet Exchange (AMS-IX)
AS1755 - EBONE
AS1759 - Telecom Finland iNET
AS1888 - CWI-Amsterdam
AS1890 - NLnet
AS2686 - IBM Global Network - EMEA
AS3215 - RAIN Reseau d'Acces a l'INternet
AS3317 - Universiteit van Amsterdam
AS5390 - EuroNet - NL
AS5417 - Demon Internet Ltd
AS5418 - Internet Exchange Europe B.V.
AS5484 - BT Netherlands Regional Service
AS5496 - Wirehub! Internet
AS5506 - The Digital City

Mail communications security will be provided by PGP and/or PEM as required by the user community. Voice communications security will be studied. More detailed specification of the current plans is beyond the scope of this document.

After Hours Availability

We have an excellent infrastructure for and ample experience and with working remotely either from home or when on travel. This is an excellent basis for after hours availability. We also have a programmable voice response system and our operational staff carry personal pagers which are triggered automatically when operational problems occur.

While we expect to provide a sufficient level of emergency access after hours, we strongly believe it would be counterproductive to suggest this being anything near 24x7 availability. Given the staffing levels of the pilot we can only provide this on a best-effort basis. We do not expect high demand for real 24x7 service since most customers currently do not have the full capability for this either. Should this demand and the preparedness to pay for it grow, we will be able to provide it given our present infrastructure.

In the meantime after hours availability for customers will be organised in one of two ways: either using filtering through an answering service or through giving selected customers direct access to duty staff. We expect to employ the latter method at first, putting the decision whether after hours access is needed with the customers. As the customer base grows we expect to switch to an in-house filtering process.

5. Financial Plan

Operating Costs

The operating costs for the SIRCE project can be thought on in terms of three budget lines, namely those for personnel, infrastructure, and NCC support. Salary and recruitment costs contribute to the personnel budget line. The budget line for infrastructure accounts for from computer, rent, furniture, office supplies, telephone, connectivity, consulting, travel and general costs. NCC support involves supervisory manager support, accounting support, and administrative support costs. The budgets for 1997 and 1998 are shown below.

SIRCE Pilot Project Budget		
	1997 kECU	1998 kECU
Personnel	154	232
Infrastructure	108	136
NCC support	24	15
TOTAL	286	383

Although we have included the budgeted costs for 1998, we would like to stress that these are very much hypothetical since it is too early to know how the project will develop in 1998.

6. Open Issues

Project Management

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 useful for ISPs. They also have significant support from existing IRTs.

Customer Involvement

Input from customers will be gained by establishing an advisory group, and by holding meetings open to all contributing IRTs. The advisory group should consist of representatives from paying customers and invited experts. Depending on the community of paying customers this should be associated with an existing organisation such as FIRST and/or RIPE.

Funding

We believe funding of the pilot project should not be left entirely to TERENA. Rather, SIRCE should be primarily funded by the ISPs from the outset. This is to establish that a clear interest in these services in the ISP community. Secondary reasons are to establish influence by the target community in the project's earliest phases and to facilitate transition to a normal service.

We also believe that the level of resources for the pilot envisioned by TERENA is lower than what will be needed to guarantee a successful service for the size of community we expect.

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". Our project plan is is designed to provide an operational service by Q1/1998.

As mentioned elsewhere in this document, the benefits for those that contribute to 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 the pilot project;

- Public credit for their contribution.

Ideally, all customers currently served by the RIPE NCC would take part in funding the SIRCE pilot. If this were the case in 1997, then the cost per customer would be ECU 365. This clearly demonstrates that it is very realistic to turn SIRCE into a regular service quite quickly.

Since we are considering a new pilot service, we cannot assume that all NCC customers will take part in funding this effort. Assuming equal contributions, the cost for those that do support this service will be higher than ECU 365. Assuming 40% of the local IRs serviced by the RIPE NCC participate in funding this project, then the average contribution per contributor will be roughly ECU 1000. Actually it can be lower depending on how much funding TERENA will be able to raise.

Given the numbers above we will request all current NCC customers to commit funding this project with a minimum of ECU 500 for 1997. During the coming weeks we will regularly publish the level of commitments received. Once we have received sufficient commitments and TERENA agrees to implement this proposal we will discuss details with them. If we do not receive sufficient commitments by November 27th we will withdraw this proposal. Should the project start, the contributions committed will be invoiced in the first quarter 1997. Should the project be oversubscribed, the amounts invoiced will be reduced pro rata.

In the unlikely case that there will not be significant funding commitments from the ISP community, we will have to conclude that interest is not sufficient and withdraw this proposal.

7. Why SIRCE at the RIPE NCC?

We believe the NCC is uniquely suited to succeed in making the SIRCE project meet its goals. In this final section, we outline the primary reasons we believe the SIRCE pilot project will prove an effective approach to the coordination of security incidents in Europe if based at the RIPE NCC.

The RIPE NCC, being a Network Coordination Center has extensive experience in the kinds of tasks to be performed in the SIRCE project and in performing them successfully at the scale which will soon be required. For example, we already organise three international meetings per year attended by members of the European Internet community. We also provide extensive information services (WWW, FTP, and mail server), the primary users of which the ISPs in Europe. Moreover, we have a solid track record of piloting services and turning them into stable and reliable operational services.

As necessary to perform its current services, the NCC satisfies all the connectivity and infrastructure requirements necessary for the SIRCE project. Because many of the tools in place to facilitate IP registration can be extended to provide SIRCE services, it is feasible to provide basic incident coordination early in the pilot project.

We also have an international group of highly motivated and competent people including those experienced in systems/network operations and security.

Most importantly, the NCC is already a focal point for the European Internet community. The customer base of the NCC consists of most European ISPs. Because the ISPs are the key Internet user contact points, they must be involved if security incidents are to be handled effectively in the European region. The RIPE NCC is in a unique position to facilitate ISP involvement, having already established a trusted working relationship with members of most ISPs and is fully accepted as neutral and impartial body in the European Internet community.

We know how to do large scale coordination. We know how to set up pilot projects and turn them into successful services.