The DFN-CERT Experience: Building up a new CERT within Europe

Klaus-Peter Kossakowski <kossakowski@informatik.uni-hamburg.de>

Abstract

Many papers about Computer Security Incident Handling have been published in the past [1,4,10]. Therefore the goal of this paper is to concentrate on the practical implications of the DFN-CERT - the Computer Emergency Response Team (CERT) for the German Research Network. Our experiences, our problems, and the lessons learned are presented. In addition, we will describe some recommendations concerning the future development of incident response teams within Europe, emphasizing the importance of a cooperative approach.

I. Introduction

Since January 1993 the Computer Emergency Response Team for the German Research Network (»Deutsches Forschungsnetz« - DFN) has been responsible for more than 400 sites - independent administration units like universities and their departments, research centers, and public sites. It is funded by the German Ministry of Research and Technology. Although the formal constituency is characterized by a network connection to the German Research Network, we provide our information to the whole Internet and serve as a clearing house for incidents within Germany on an international scale.

Throughout the past year we have observed a growing number of incidents and vulnerabilities. Our main task is to address this situation and help the local site administrators to avoid incidents, and to act quickly and efficiently as new incidents are detected. Of course we help them by clearing up their systems after an incident has occurred, and give direct assistance while an incident goes on. As the DFN-CERT was started as a research project much effort was spent determining the attitude of our user community to a Computer Emergency Response Team for their network.

As one of the few CERTs within Europe we are very interested in the development of a suitable and efficient infrastructure for Computer Security Incident Handling within the European part of the worldwide network. As approximately 25% of the Internet hosts are now located in Europe, we see the need for a European CERT Coordination Center in order to address this growth and the expected corresponding growth of European CERTs.

II. Computer Security Incident Handling

The concept of teams which help a user community (their constituency) in case of computer security incidents has proven to be successful, since the first teams - CERT/CC and CIAC - were formed after the Internet worm of November 1988 [2, 5, 9]. Notwithstanding such dramatic events, the usual work of CERTs is more often related to ordinary problems. However, simple administrative failures and lack of awareness can lead to the same damage as a rogue program. Instead of concentrating only on handling real incidents, much effort must be contributed to avoid incidents and warn users when new vulnerabilities are exploited.

Many other teams were formed since 1988 and there has been a growing need for cooperation, coordination, and trusted communication between them as incident response was recognized as an international problem [7]. FIRST, the Forum of Incident Response and Security Teams, was formed to address these problems [3]. The CERT Coordination Center (formerly known as CERT/CC) and CIAC (Computer Incident Advisory Capability) were among the initial members of FIRST. Today FIRST has more than 30 members, six of them in Europe, one in Australia.

III. Establishing the DFN-CERT

The DFN-Verein, as the network provider for the German Research Network became involved with Computer Security Incident Handling, because a RARE Working Group addressed the need for CERTs within Europe. They decided to set up a CERT as a research project to determine the pros and cons of this concept for the DFN. The team began its work in January 1993, nearly six month before the RARE CERT Task Force was set up to influence the European development of CERTs.

The team is located at the Computer Science Department, University of Hamburg. It is sponsored by the German Ministry of Research and Technology. The team currently consists of two scientists and the director of the Computer Science Department. The aims of the DFN-CERT are:

- assisting the members of the German research network in setting up preventive measures to improve the security of the participating sites
- giving quick and effective help and information in case of security related incidents
- intensifying the flow of information between the DFN-CERT and similar international groups and establish a reliable cooperation
- setting up contacts with vendors and software distributors for the exchange of security related information
- designing concepts for a future full operational DFN-CERT

Since we started our work we were especially concerned with building up our constituency. Because we were set up from the network provider we had to fight to become well known and accepted by the user community. Therefore we presented our project at various meetings and announced our services via user magazines, email, and netnews. In the meantime a growing number of reports and requests has been addressed to us. Various administrators were very helpful at the beginning as they provided critical information to us, only in hope of finding some kind of support. After that they carried out their experience to other sites and we have gotten involved in more and more cases. If confidential information has been given to us, the distribution of this information will necessitate the consent of the originator. The removal of identifying data will be used for further protection of persons or sites. Sensitive information will be sent via electronic mail only with the help of cryptographic methods.

In the beginning we spent a great amount of time with an inquiry to all sites within our constituency. This was possible, because it is a well known and closed group of X.25 and IP sites. We got 70 answers (from 330 requests) and used the information for two purposes: first we got a list of trustworthy site security contacts, and second we got more information about the interconnectivity (e. g. use of modems and protocols/services), the systems, their information sources and - most important for our task - their attitude towards DFN-CERT and CERTs in general. With a feedback of more than 20% we got a good impression of their situation and their expections as to what we should do as »their« CERT. (Some of the results are presented in section IV.)

We were involved in various vulnerabilities and shared our information with other CERTs. In the past we have provided our expertise in some serious events like the expreserve-, the gopher-, and sendmail-vulnerabilities. We learned from this cooperation and were accepted by other teams. As they became more familiar with our team, they encouraged our membership by FIRST. The membership in FIRST enables a trusted cooperation and the use of critical information from other teams.

To warn our constituency we maintain a mailing list of site security contacts to distribute our *Security Bulletin*. In case we were not involved in an analysis we forward the original advisories and bulletins from other teams which we get through the FIRST communication.

We searched for efficient and easy-to-use ways to distribute information. The traditional way was to use an AnonFTP service. We started this service in January and used an already existing subdirectory of our local computer center (directory /pub/security on ftp.informatik.uni-hamburg.de)

As one of our team members is interested in wide area information systems we used his experience and provided a GOPHER server since July 1993 (gopher.informatik.uni-hamburg.de). We decided to provide the same files and information as stored on our AnonFTP server, except the software directories, but we used the enhanced features: descriptive headlines for the single files and a search engine for full text retrieval based on the WAIS package.

As we had to prepare additional reports (about topics like computer security education and projects at german universities, information sources, and the legal situation) we had no time to develop our own security tools. Instead, we used our resources to provide technical guidelines for firewalls and well known security tools. For this purpose we distributed several *Information Bulletins* and technical reports.

IV. Lessons Learned

Although we tried to read all papers about CERTs and their work, we had to learn many things related to this kind of work by ourselves. We got much helpful information from administrators within

our constituency, through the inquiry, and from other CERTs. All this provided us with the necessary knowledge to bring the project to a successful end - preparing the future for a full operational DFN-CERT.

Looking back the DFN-CERT got involved with real incidents sooner than expected. And it took us more time than we had expected to track these incidents down. When we first prepared our plans for the project, we felt that we should provide incident handling capability instead of only doing a research project. This decision was right, but we were surprised at how difficult it was to coordinate the research tasks with the more and more emerging need for incident handling, vulnerability analysis and support for system administrators.

This involvement, however, gave us the right impression of what tasks a DFN-CERT has to address. Without this experience we would have prepared a well behaving but worthless project for the future.

As a research project we had no other duties than to fulfill the needs of the DFN-CERT. This situation is totally different from other European CERTs: often the members are employed by the network provider and work only part-time on this topic (e. g. CERT-NL). Only this independency allowed us to finish our research task, to handle incidents as they occur, to do vulnerability analysis and spend the time for the information services.

Perhaps the most important - and difficult - topic is the ongoing process to build up a constituency and to communicate the services and advantages to this community. It is difficult to build up a trusted relationship to a large community from the ground up. A fact which helped us was that our director is well known in the German Research Network. This gave us the basis to begin the communication with many sites.

We took advantages of being employed by a computer center, which has the same problems as any other site in the German Research Network. So we learned from their experience and helped them to improve their own security procedures. These experiences were very helpful in providing guidance to our community.

To be accepted by other CERTs is a very important topic. Without a trusted relationship and methods to protect the communication channel there is no chance to exchange critical information about sites, vulnerabilities or ongoing developments. The only way to build up such relationships is to meet other CERTs personally. Looking back, the fact that we became a member of FIRST changed our work dramatically. Since that day we receive all the information CERTs are willing to share with other teams. This provided us with very important information and helped us to care for our constituency. It opened a door to other well known experts in the field of network and computer security, too. This is perhaps the biggest advantage, because we can not (like most of the different teams) provide the whole technical background which is necessary for our constituency. As a new CERT we took advantage of the already established cooperation between vendors and other teams, but we think it is very important to have our own contacts with the national representations.

The need for cooperation on a worldwide scale can not be underestimated. Since our work started we have dealt with incidents from many foreign countries, and german hackers were active in many countries, too. As a CERT for a single network it is even difficult to get a realistic impression about the ongoing development. Without the communication and exchange of information it is unlikely that a single team can determine the global figure. But without this knowledge (sometimes derived from the so called technology watch) no CERT can address the real needs for its constituency. The knowledge must be used to raise the awareness of the constituency. Only if we as a CERT can address the emerging threats before incidents occur we will get a chance to avoid these incidents - and every incident takes some of our time, which can not be used to provide assistance to the community and therefore will lead at last to new incidents.

As we as a CERT are known as the »good boys« it seems natural to become a target for the »bad boys«. This means we must be prepared for the worst case. Because our work depends on reachability via email and services like AnonFTP and GOPHER, we are connected to the network. Since we use the same basic technologies (e. g. workstations, PCs) we are vulnerable whenever a new bug is discovered in an application or operating system. I remember the day very well as we learned about the potential threat that every user could exploit a bug in the GOPHER server to execute commands. We spend much time on the administration of our systems and try to use new concepts and techniques to enhance security (e. g. PEM and Firewalls). But there remains a small risk, so we

decided to delete critical information as soon as possible and to store the information on unreachable systems. To avoid a total dependence on the network we collect telephone and telefax numbers of our site security contacts and other CERTs in order to be prepared for a real network emergency.

From our experience we learned that we had to address some other topics as well. Good and direct relations with various network providers and law enforcement are important and necessary. The DFN-CERT will never announce a site specific problem to the police but contact information is important in order to act quickly when a hacker case is observed and the site decides to go to court. In some actual cases there was the need for tracing various calls which is almost impossible without the help from the public network provider.

By providing information, computer security related reports, and past advisories from the various CERTs we found that our GOPHER server was more often used than the AnonFTP server. In 1993 we counted approximately 20.000 accesses to this server. We observed the same amount of accesses in the second part of the year for our GOPHER server. The conclusion is to concentrate on the AnonFTP server for tools and software packages and to provide other files with full text databases via the GOPHER server. We are planning to use new information services like XMosaic to provide a more interactive access to the information (perhaps like an on-line tutorial about computer security).

At the end of this chapter a short summary of the results of our inquiry should be given. Concentrating on the important facts for our work, comments are given which reflect our practical experience.

Most of the sites (nearly 70%) need assistance for workstations and mainframes with UNIX as operating system. Many sites have already noticed incidents with UNIX systems (e. g. passwords, automatic programs). In fact, most of our incident handling and vulnerability analysis was concerned with UNIX systems.

Besides this, system support for PCs are recommended by 30% of the sites. The only real threats in this area seem to be computer viruses and the theft of hardware. We address viruses by providing general guidelines and contacts to the MicroBit-Virus-Center (University of Karlsruhe).

We asked the sites to send us their computer security policies (if available). We got one policy from one site. Almost all other sites are either really interested or on the way to establish their own policies. In fact, we identified this topic as an urgent task for the near future. As we have seen in the past, without an explicit policy it is nearly impossible to establish efficient, new security procedures or technologies.

One question has contributed to the services of the DFN-CERT. Almost all sites wish to get: alerts, warnings about upcoming threats and information about information sources. Nearly 50% wish additional tutorials or workshops to learn more about site administration and security tools. In spring of 1994 the DFN-CERT has offered a workshop for interested administrators and tutorials are planned for the future.

In case of an incident, information is the most important topic for all sites together with contact information (e. g. vendors, police). Only 30% believe that the analysis of the incident is necessary and 15% would like local assistance. The DFN-CERT has no plan to provide local assistance and it seems not necessary to analyse all incidents in a deep detail. But sometimes it can be of vital interest for all CERTs to learn more about the technological knowledge of the hacker community.

V. The European Development

The future development of Computer Security Incident Handling Teams within Europe is one of the most challenging topic in this field. The establishment of the RARE CERT Task Force is the most visible event and it emphasizes the need for a European effort. Their interesting tasks are the »Campaign to persuade all European networks to set up CERTs and to join FIRST […]« and »Co-ordinate the creation of an organizational structure within and between European networks […]« [8].

As a result of the evolving network infrastructure within Europe there is a growing need for Computer Security Incident Handling Capabilities. As we see in the actual statistic of October 1993, the increase of Internet hosts in Europe is 117% in 1993. In fact this is one of the biggest increase worldwide and approximately 25% of all hosts are now located in Europe.

There are many networks within Europe and only a few have an own CERT. Up to now there is no organisation within Europe which coordinates different teams or oversees the situation. There are only a few trusted relationships between the different teams, there are no procedures for including new

teams and the communication concentrates on the exchange of incident information. Not all teams are members of FIRST, so there is a different level of information and knowledge exchange.

In this situation we have the following recommendations:

- use FIRST as an already established forum with similar interests
- build up a European forum within FIRST (SIG Europe)
- communicate common problems and characteristics to other teams worldwide but emphasize (if necessary) the specific European topics
- enable the participation of other teams in SIG EUROPE as they are interested in the European situation
- integrate new teams and help all teams to fulfill their goals
- build up trusted relationships between all teams and support the cooperation with non-European teams

With the growing number of new CERTs it seems very unlikely that there can be a trusted relationship between all teams (even within Europe). So the need for a central clearing house is obvious. Nowadays the CERT Coordination Center fulfills exactly this position. If we don't know another team, we use their communication channels. Without this central coordination every team has to do all technical analysis by itself or has to figure out if this is an already known vulnerability.

Building up an additional level of hierarchy is not easy. There are some disadvantages but on the other hand there are reasonable advantages for a European CERT Coordination Center:

- it can cooperate on the same level with the CERT Coordination Center
- it can care for the European part of the world and is located in the same timezone
- it is aware of the specific details of the European situation and special regional problems
- it can build trusted relationships to all European teams and can act as a European clearing house

This team must be responsible for all other European networks and teams. All teams will serve for their constituency, but some of their work will be coordinated and supported by this new center. It seems natural that in the future we will find teams for military, government, commercial, public and research networks in most of the countries. Therefore the team must be relativly independent to guarantee the confidentiality and the responsible function without (political) influence from any side.

Before we can try to establish this coordination center there must be a clear understanding of the tasks and goals with respect to all requirements of all teams. This is very difficult since today only a few teams can participate in this effort and we must make decisions for the future. A working group has been established to provide recommendations and to address the various problems that must be solved.

VI. Conclusion

Our plans for the future are based on our experiences. We are planning a new structure with three scientists to address the main topics: management, vulnerability analysis and incident handling. Together, we will maintain our global information services.

We will expand our services by providing tutorials offering information and assistance in the implementation and administration of improved security technologies and techniques. And we will address the urgent need for computer security policies by providing guidelines and assistance.

While we will not address the development of new tools, we will do research work on important topics, like firewalls, and distribute guidelines for the use of security tools.

DFN-CERT's development as an organization has not always been easy, but it has shown to be successful. Fully accepted in the international community, we have received, over time, more and more reports from german sites, and have succeeded in building up our constituency.

As we see ourselves as an integral part of the worldwide community of network users, we have become involved with the European development. We hope that with new CERTs within Europe and a European CERT Coordination Center the emerging threats can be addressed.

As an active member of the working group that will provide recommendations for a European CERT Coordination Center, I will personally care for the practical concerns of cooperating CERTs.

We know how difficult it can be to establish a new CERT and we are willing to share our experiences with other groups. We would be glad to provide information for setting up their own CERT and we can act as a sponsor for a FIRST membership.

We have gained a good understanding of what a DFN-CERT should ideally be, and we have made plans for the next phase of this project. We hope we can address all the requirements of our constituency with the new structure and our services, and that we are able to participate in the worldwide task of preventing computer security incidents in the future, just as we have done in the last 18 months.

VII. References

[1] R. Brand, Coping with the Threat of Computer Security Incidents.

[2] DARPA, DARPA establishes Computer Emergency Response Team, December 1988.

[3] FIRST / Operational Framework.

[4] K. Fithen and B. Fraser, CERT Incident Response and the Internet, INET'93, pp. EEC:1-7.

[5] B. Fraser and R. Pethia, The CERT/CC Experience: Past, Present, and Future, INET'92, pp. 203-208.

[6] P. Holbrook and J. Reynolds, Site Security Handbook, RFC 1244.

[7] R. Pethia and K. van Wyk, Computer Emergency Response: An International Problem.

[8] RARE CERT Task Force, Guide to setting up a CERT.

[9] E. Schultz, DOE's Computer Incident Advisory Capability (CIAC).

[10] J. Wack, Establishing a Computer Security Incident Response Capability (CSIRC), NIST Special Publication 800-3.

Acknowlegment

I would like to express my thanksfulness to the CERT Coordination Center and the people in this team. They gave me the chance to learn more about our task and as a sponsor for our FIRST membership they helped our project to be successful.

Author Information

Klaus-Peter Kossakowski is a member of the Internet Society and the German Gesellschaft für Informatik - GI.

He has earned a diploma from the University of Hamburg in the field of Information Science. His studies concentrated on networks, communication and computer security.

Prior to joining the DFN-CERT Peter was a system programmer for ISDN network services and applications.

The DFN-CERT can be reached via e-mail: dfncert@informatik.uni-hamburg.de. The team is located at the University of Hamburg / Computer Science Department (Vogt-Kölln-Straße 30, D-22527 Hamburg, Germany).