MD-CERT Services for Scientific and Research Communities of Moldova

Alexei Altuhov, Peter Bogatencov, Alexandr Golubev, Veaceslav Sidorenco
RENAM
bogatencov@renam.md, galex@renam.md, alexx@renam.md, svv@renam.md

Abstract

Paper describes details of MD-CERT: new Computer Emergency Response Team services created in order to register, monitor and avoid dangerous security incidents in the RENAM's network. This is a group of specialists who should engage in registration incidents in the network and assist in eliminating their consequences. MD-CERT - is a center of internet security expertise, located at the RENAM, Research and Education Networking Association of Moldova that study internet security vulnerabilities, research long-term changes in networked systems, and develop information and training to help to improve security level.

1. Introduction

MD-CERT it is the center of computer incidents analyzing. MD-CERT is engaged in gathering and analyzing of the facts of computer incidents (i.e. attempts or the facts of infringements obviously certain by the owner of the information or standard in a network the Internet corrected works with computer resources), concerning to the network resources located in territory of Moldova.

Any information about computer incidents, references to useful resources in the field of protection of information technologies, wishes, will be closely considered and as far as possible taken under consideration. MD-CERT guarantees confidentiality of all sent information on incidents. MD-CERT is the noncommercial project and according to this status is not engaged in the activity connected with advertising, promotion of those or other decisions and techniques, an exchange of banners, development of projects on protection, etc.

Realization of CERT in Moldova is sponsored by NATO project "Creation of Infrastructure for CERTs in Belarus, Moldova, Ukraine and their Initial Operation" in R&E networking segment of Moldova.

Specific features of RENAM CERT organization and functioning:

- RENAM CERT deploying is effectuating in close cooperation with national CERT coordinator – "The Center of Special Telecommunications";
- NREN CERT is a part of the creation national structure of Secure Incident Response Centers;
- RENAM CERT personal training plans include activities at the local level and participation in international training events.

2. RENAM communication infrastructure development

Basic communication infrastructure development has to be accompanied by realization of two principal approaches that affect the networks utility and end users' quality of services:

- New networking and informational services deployment
- Secure and reliable network operation, operative reaction on any security incident

Under 'New networking and informational services deployment' we understand deployment od the RENAM networking and creating new services for increasing the usability and affectivity of the RENAM network.

But it is only one path of the RENAM activity. Another path is increasing the level of security in the RENAM's user's community and guarantees confidentiality of information for RENAM users. In order to make RENAM network more secure was created a CERT for providing new security technologies in the Moldavian's network community. The main principles of CERT creation are:

- Security technologies implementation
- Organizational measures.

3. CERT Services

There is a lot of software what can be useful for a CERT team in their activities. All of them provide the following idea that CERT activity may consist of any or all of:

- Incident prevention
- Incident detection
- Incident analysis
- Forensic evidence collection

- Tracing or tracking
- Incident post-processing.

In order to provide this result exist some services what are shown in the list below.

Reactive Services

- Alerts and Warnings
- Incident Handling
- Incident analysis
- Incident response on site
- Incident response support
- Incident response coordination
- Vulnerability Handling
- Vulnerability analysis
- Vulnerability response
- Vulnerability response coordination

Proactive Services

- Announcements
- Technology Watch
- Security Audits or Assessments
- Configuration and
- Maintenance of Security
- Development of Security Tools
- Intrusion Detection Services
- Security-Related Information Dissemination

Artifact Handling

- Artifact analysis
- Artifact response
- Artifact response coordination

Security Quality Management

- Risk Analysis
- Business Continuity and Disaster Recovery
- Security Consulting
- Awareness Building
- Education/Training
- Product Evaluation or Certification

4. CERT services in RENAM

In order to provide CERT Services at the RENAM community and network a CERT server was set up that hosts the CERT web site, incidents databases and other facilities (fig 1.).

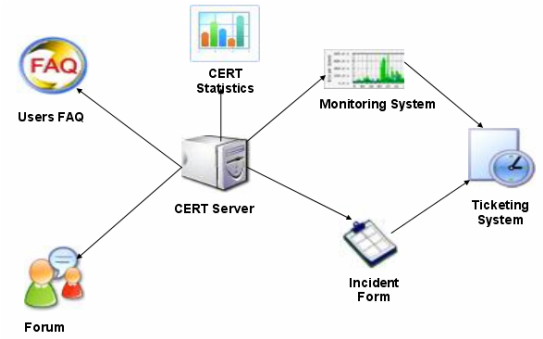

Figure 1. CERT Server.

This Server must provide the next services to RENAM users:

- Incident form
- Forum
- FAQ
- Links
- Statistics
- Mail to CERT Officer.

Using these Server CERT Officers can access the next services and possibilities:

- Collecting incidents
- Making statistics
- Alerting the constituency.

5. Collecting of the incidents

Collecting of the information about the incidents should be done by at least 3 methods:

- Monitoring of the network and fixation of its suspicious parts or actions in the network.
- User will inform by himself about the incident on his part of the network and after this information is processed by CERT officer it will be considered as an incident.
- Information about the incident can be received from another CERT system, because these systems and teams must exchange information about the incidents.

In the first case the incident is fixing automatically with help of many software programs and hardware equipment, mostly with help of such protocols as ICMP SNMP. A lot of software for monitoring network systems does exist, for example NAGIOS and NetIIS. These programs are comfortable and well tested, but not always are suitable to all requests of monitoring. Also there is the necessity for CERT officers to add some modules for monitoring system.

Fixation of the incidents via automatic facility of monitoring helps to define existing of the incidents and

even avoid the incident automatically. Besides this the automatic system helps to define statistics and consequence of the incidents and make action to avoid it.

The incident also can be examined by CERT officer if the incident is registered and sent to CERT officer via one of these methods:

- Phone
- Fax
- Registered on the site CERT - cert.acad.md, cert.renam.md, www.cert.md
- Sent via e-mail – inc@cert.md
- Sending the information about incident using other means.

In this case as in the case of automatic registration of incident on each incident opens a ticket and it register in "Ticketing system".

The ticket should be examined by one of the CERT officer during one day and if this CERT officer will consider that this is real incident the ticket will be appropriated corresponding priority and information about registering this incident will be sent to user. It means that this incident is already examined by CERT officer. At this time CERT will strive to handle this incident and after successful resolving of the incident this user also will be informed about the result of incident and also will get a manual about avoiding this incident in the future.

For help in elimination of the incident to the CERT officer could ask not only users but also system administrator of the network that CERT is serving and systems administrators of other CERTs as at national and at international level. Either every CERT should inform each other about danger of incident and assist to each other in its handling.

MD-CERT first is functioning for the interests of scientists, education staffs and students of Republic of Moldova, though his users can be any people that have any attitude to the computer incidents. The priority in examining of the incidents and assisting in consultation have the users of RENAM network.

6. Statistics

MD CERT services are collecting a set of valuable statistics:

- General statistic available for every user
- Statistics for incidents occurred monthly grouped by types
- Statistics for incidents that were resolved (handled) by CERT officer, for analysing the work of every CERT officer.

There must be one another SOAP service that shows the daily and month statistics for publishing on another sites or Newspapers.

7. Conclusions

MD-CERT is set up and running. RENAM users and administrators have the main priority in resolving and analysing the incidents. But all the Internet users from Moldova and from other countries can use the CERT services of RENAM Association for resolving the incidents in their network segments. Another important fact is that increasing of network security depends not only from CERT officers but all the system administrators and user of all Internet community.

8. References

[1]. A Step-by-step Approach on How to Set Up a CSIRT. European Network and information Security Agency (ENISA), 2006.

[2]. A. Altuhov, A. Golubev, S. Savchik, et al. "Computer Emergency Response Team", RENAM National Research and Education Network User's Conference. 2007.

[3]. A. Altuhov, P. Bogatencov, A. Golubev, V. Sidorenco, "Development of services for analysis and prevention of incidents in RENAM network", V International Conference on Microelectronics and Computer Science, Chisinau, 2007.