

# MD CERT In RENAM Network

**Alexandr Golubev**  
(E-mail: [galex@renam.md](mailto:galex@renam.md))

**RENAM Association**

**[www.cert.md](http://www.cert.md)**

**[www.renam.md](http://www.renam.md)**

**RENAM – Research and Educational Network Association from Moldova.**

**RENAM network is providing services for scientific and educational organizations, personal members of scientific – educational community of Moldova.**

**At the moment, more than 80.000 users, working in more than 30 organizations, make use of RENAM facilities. 20.000 workstations, personal computers and 100 servers operate in the net. RENAM has peering agreements with some principal Internet Service providers in Moldova.**

# CERT in Moldova

**Realization of CERT – 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 MD CERT organization and functioning:**

**MD CERT deploying is effectuating in close cooperation with national CERT coordinator – SE “The Centre of Special Telecommunications”;**

**MD CERT is a part of the creation national structure of Secure Incident Response Centres;**

RENAM CERT starts in January 2007

01.12.2006 - installed the hardware 1 server and 1 workstation

01.01.2007 - created a web page on [www.cert.md](http://www.cert.md)

End of 2007 - installed and configured ticketing system RT.

October 2007 - the first incident from another CERT– from CERT Polska

05.03.2008 - registered first incident from another CERT in RT ticketing system.

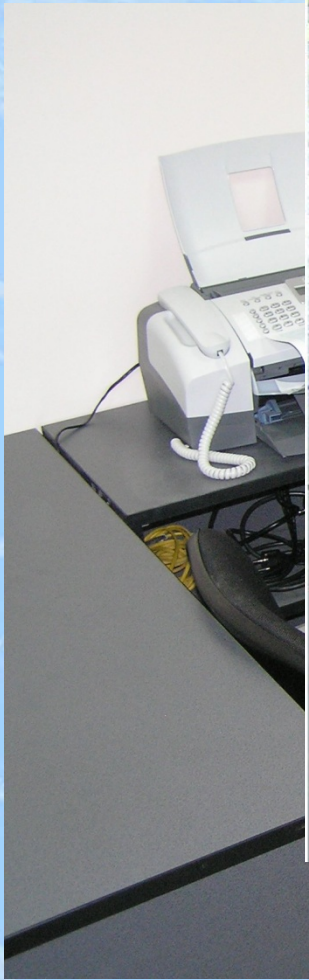
01.01.2009 – finalized NATO project “Creation of Infrastructure for CERTs in Belarus, Moldova, Ukraine and their Initial Operation”

02.06.2009 – CLOSER Workshop at Chisinau.

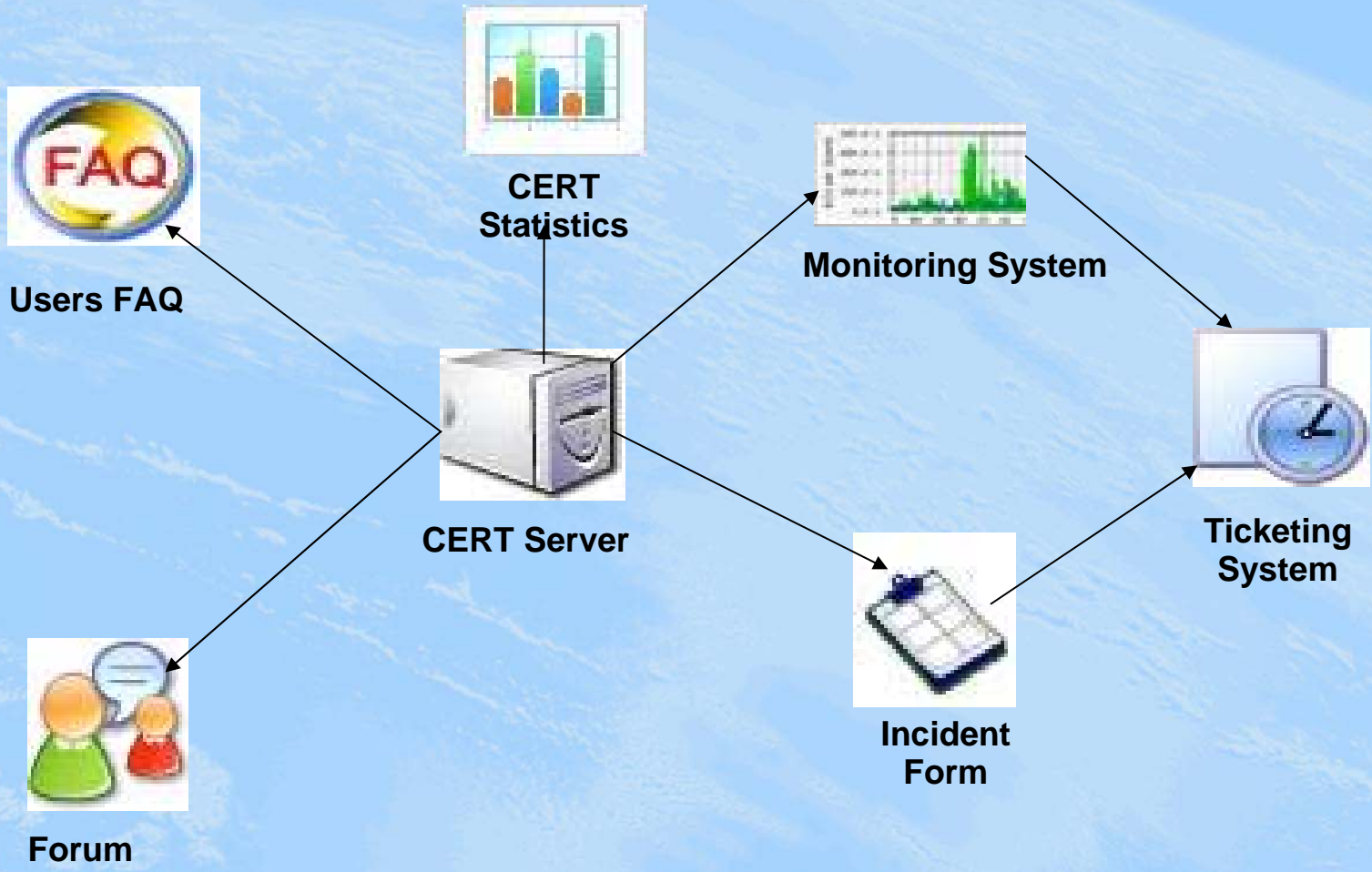
21.06.2010 – sent request to be listed in trusted introducer list

10.09.2010 – finalized cert.md web site redesign

Cert



# MD CERT Structure



- Cert-RENAM web page [www.cert.md](http://www.cert.md)
- Mail for incidents [inc@cert.acad.md](mailto:inc@cert.acad.md)
- Form for submit: <http://cert.acad.md/submit-an-incident>
- Trace incident: <http://cert.acad.md/trace-incident>

## CERT Web Site – www.cert.md

### MD CERT

HOME | OUR RULES | NEWS | EVENTS | PUBLICATIONS |

Center of internet security expertise  
located at the RENAM Network



MD-CERT - CERT is a center of internet security expertise, located at the RENAM, Research and Education National Association from Moldova. We study internet security vulnerabilities, research long-term changes in networked systems, and develop information and training to help you improve security.

MD-CERT it is the center of computer incidents analyzing. MD-CERT is officially registered CSIRT (Computer Security Incident Response Team) center and 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 MD. 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.

- Submit an Incident
- Email Incident
- FAQs
- Contact Us
- Trace Incident

For increasing security and registration dangerous incidents in the RENAM's network was created CERT (Computer Emergency Response Team). This is group of specialist who should engage in registration these incidents in the network and assist in eliminating the incidents.

Collecting of the information about the incidents should be done by 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. There is a much of software for monitoring the system for example (Nagios and NetIIS). These programs are comfortable and well tested, but not always are suitable to all requests of monitoring. Also exists 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 this methods

- Phone
- Fax
- Registered on the site CERT - [cert.acad.md](http://cert.acad.md) , [cert.renam.md](http://cert.renam.md), [www.cert.md](http://www.cert.md)

### Latest News

CERT Forum is a place where constituency and other Users can discuss their problems and exchange the experience.

[more..](#)

### Gallery



### Poll

How DID you LEARN about MD CERT?

- From News Paper
- From Publication



# CERT-MD: State of Art

## Submit an Incident <http://cert.acad.md/submit-an-incident>

Association from Moldova. We study Internet security vulnerabilities, research long-term changes in networked systems, and develop information and training to help you improve security.

MD-CERT is the center of computer incidents analyzing. MD-CERT is officially registered CSIRT (Computer Security Incident Response Team) center and 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 MD. 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.

Submit an Incident

Email Incident

FAQs

Contact Us

First Name:

Last Name:

Email Address:



Please Describe our problem

Topic:

Please provide a short description of the incident:

Logs:

Attachments (screen grabs, or other documents that help explain the problem)

файл не выбран

### Latest News

CERT Forum is a place where constituency and other Users can discuss their problems and exchange the experience.  
[more..](#)



## Trace Incident <http://cert.acad.md/trace-incident>

MD-CERT - CERT is a center of internet security expertise, located at the RENAM, Research and Education National Association from Moldova. We study internet security vulnerabilities, research long-term changes in networked systems, and develop information and training to help you improve security.

MD-CERT it is the center of computer incidents analyzing. MD-CERT is officially registered CSIRT (Computer Security Incident Response Team) center and 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 MD. 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.

[Submit an Incident](#)

[Email Incident](#)

[FAQs](#)

[Contact Us](#)

[Trace Incident](#)

TicketID: 6313

Ticket:

[Redacted]

Created ON: 2010-09-01 10:32:35

Created by:

[Redacted]

LastUpdated: 2010-09-10 09:34:07

Assigned to: Galex

Assigned at: 2010-09-10 09:34:06

Issue Progress:

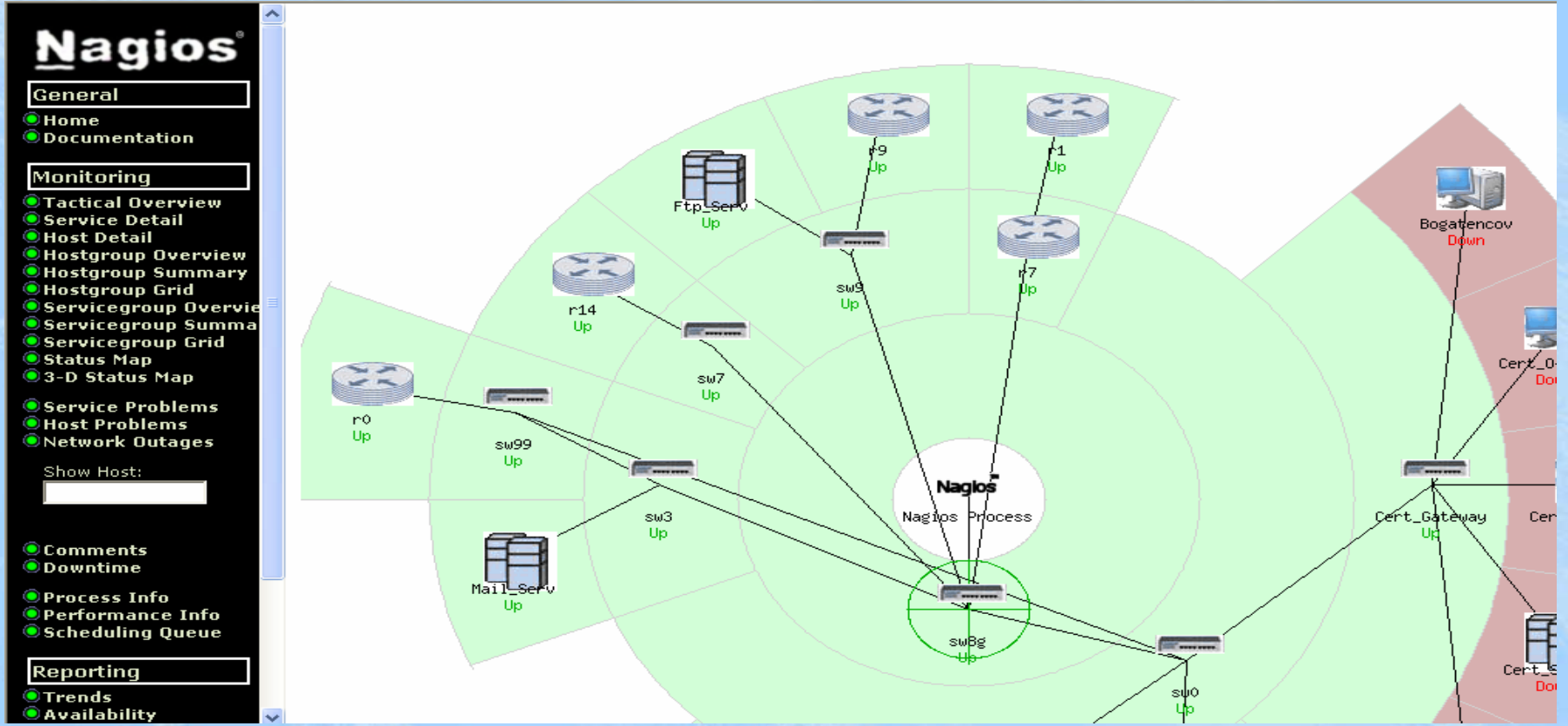
Create 2010-09-01 10:32:36

[Redacted]

Collecting of the incidents

- **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.**

## Collecting of the incidents using Nagios



The main problem is organization of dynamic collecting of the IP From RENAM network



RT for cert.renam.md

New ticket in

General

- Home
- Tickets
- Tools
- Approval

RT at a glance

X 10 highest priority tickets I own...

#	Subject	Pr
6294	(No subject)	0
6301	[101465787] Trojan Related File Found on Server ( <a href="http://deilaeyeew.ru/bin/saejuogi.bin">http://deilaeyeew.ru/bin/saejuogi.bin</a> )	0
6302	Assistance requested for additional malware scheme	0
6309	An Incident occured: Fraudulent Trojan Site Found on Server ( <a href="http://qeoimcnqoiroiwnvqnqornunoic.com/florencesd884ex48c7wbgf/florence4auq8jjvyvcp7n5fwf7d7.php">http://qeoimcnqoiroiwnvqnqornunoic.com/florencesd884ex48c7wbgf/florence4auq8jjvyvcp7n5fwf7d7.php</a> ) [BBV20100818(2)R]	0

X 10 newest unowned tickets...

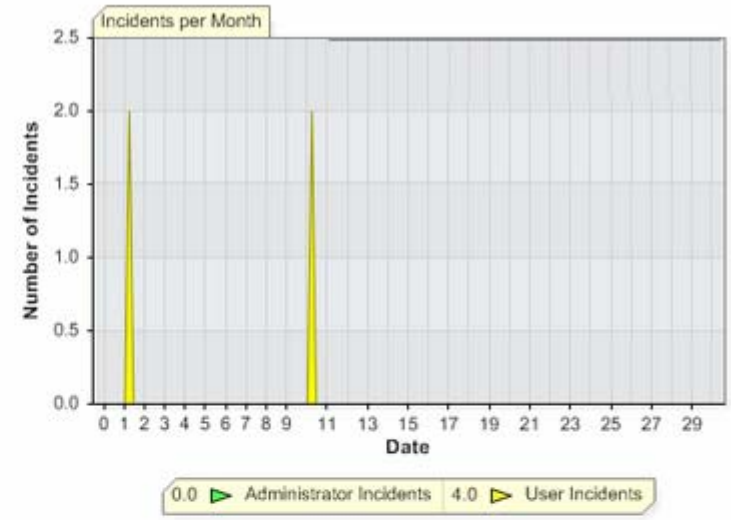
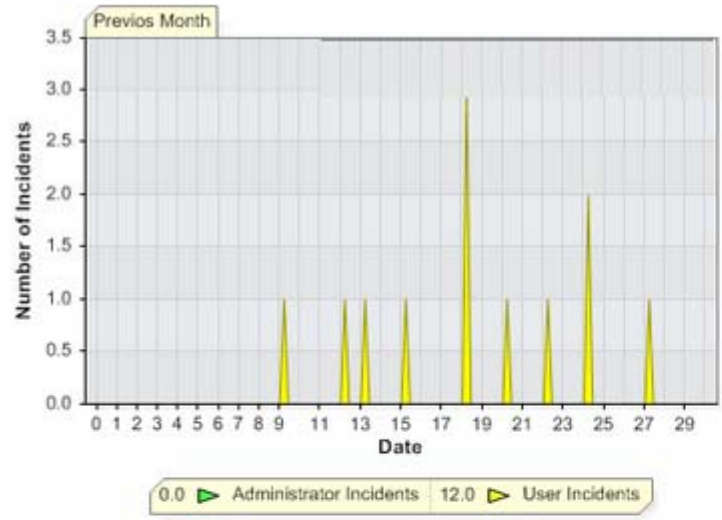
#	Subject	Queue	Status
6316	incident	Incidents	new
6315	An Incident occured: [PL-12589] Malware - 195.5.161.68	Incidents	new
6314	An Incident occured: [PL-14368] Malware - 195.206.246.203	Incidents	new

X Quick ticket creation

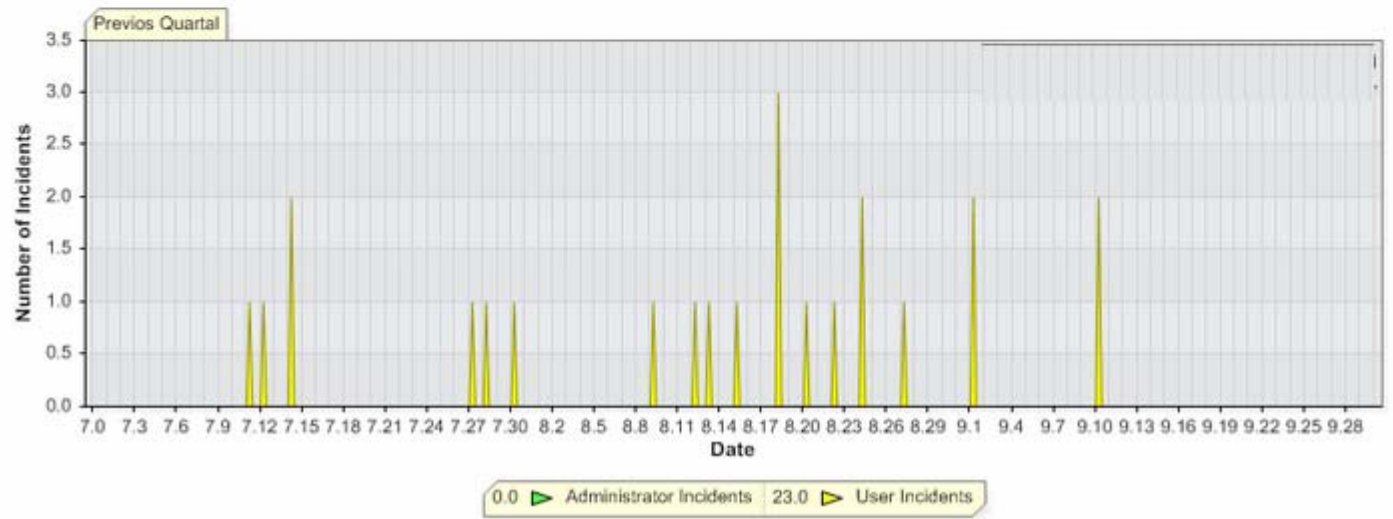
Subject:

Queue:

Owner:



CERT Quartal Statistic



Main constituency of CERT-MD are Moldavian universities – members of RENAM Association.

The main types of incidents are

- *Spam*
- *Port scanning*

In addition CERT-MD registered and helped resolving incidents from CERT's from other countries – Poland, Spain ,USA, etc...

The type of those incidents were:

- *Phishing*
- Malware Hosting

- **Incident tracking system**
- **Incident handle**
- **Software network monitoring**
- **Website with web resources**
- **Statistics**
- **Established contacts with foreign CERT teams**

**CERT problems and future plans**

**Team of CERT RENAM is looking for ways to implement more services for RENAM constituency.**

**There are 2 principal ideas how to improve work of CERT in Moldlova:**

- Creation of anti DDOS network in Moldova
- Development of CERT infrastructure in the Republic of Moldova

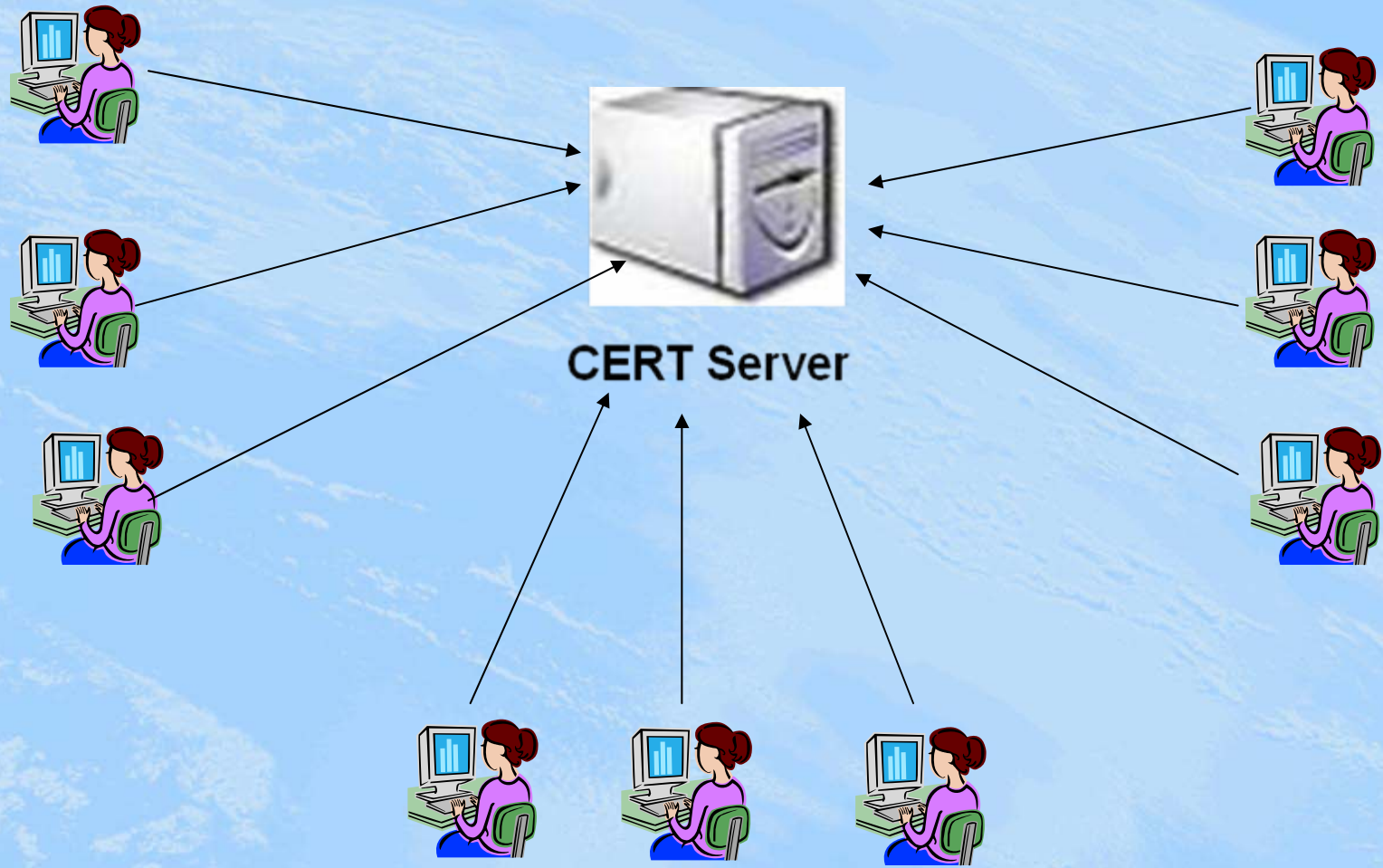
## Development of CERT infrastructure in the Republic of Moldova

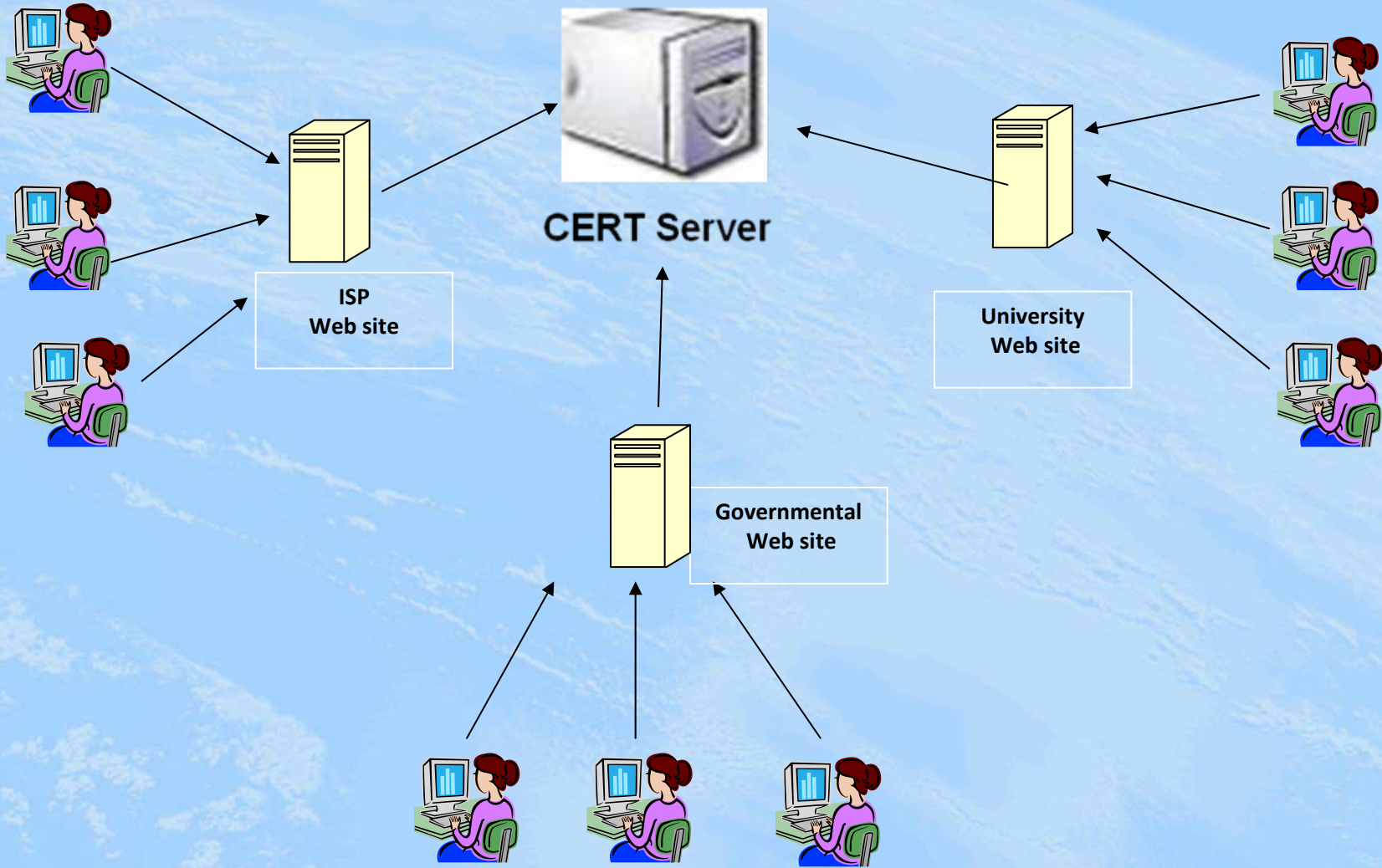
**One of the main priority aim for CERT-RENAM is spreading security technologies through all RENAM network. The high priority goal is to offer each user in the network to submit incident which will be handled by CERT.**

**Current CERT infrastructure provides different possibilities for submitting the incident, but all of them have much parameters( IP, logs, ...) that user need to introduce. It makes them not user friendly for internet Users.**

**The solution is to develop an web infrastructure:**

- Creation of common INTERNET portal for collecting and handling the incidents**
- Web module that we will be able to install at all Institutions for collecting incidents on the web sites.**





**Creation of a centralizing system for collecting incidents will offer:**

- **To localize and prevent the incident at the early step of it's spreading**
- **Track the evolution of the incident from its first appearing in the network**
- **Configure the monitoring of the dangerous parts of the network**
- **Make a wide statistics of the incidents as for the whole Republic and for selected organization.**

- 1. Improving the web site [www.cert.md](http://www.cert.md) to create the informational portal of Informational security.**
- 2. Creating the special web module that can be integrated to different web resources, with special components for collecting, analyzing, monitoring of the incidents and special tools for calculating local statistics**
- 3. Installing the web module at the all large ISP, public and governmental institutions , large educational organizations.**
- 4. Connecting the local web sites with portal using web services.**
- 5. Creating the system of common statistics**

## Creation of anti DDOS network in Moldova

Creation a system for fighting against DDOS attacks using existing governmental network infrastructure of the Republic of Moldova. DDOS is a great problem for commercial and governmental INTERNET resources in our days. There doesn't exist any universal algorithm for defending against DDOS for one server. The solution of this problem – is creation of unity distributed system for defending against DDOS based on the all servers of the republic. It will make possible to distribute identification of the legacy user threw the servers that are not attacked at this moment, that will guard the attacked server from the intruders attacks and will decrease its loading.

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.

RENAM-CERT is open for communication and cooperation with other CERT teams from Moldova and other countries