CTS

Centrul de telecomunicaţii speciale

STATE ENTERPRISE CENTER OF SPECIAL TELECOMMUNICATIONS

CYBER SECURITY CENTER CERT-GOV-MD

BUILDING AN EFFECTIVE NATIONAL CSIRT

Natalia Spinu

Head of CSC CERT-GOV-MD

Cybersecurity conference, Turkey, Istanbul, October 2015

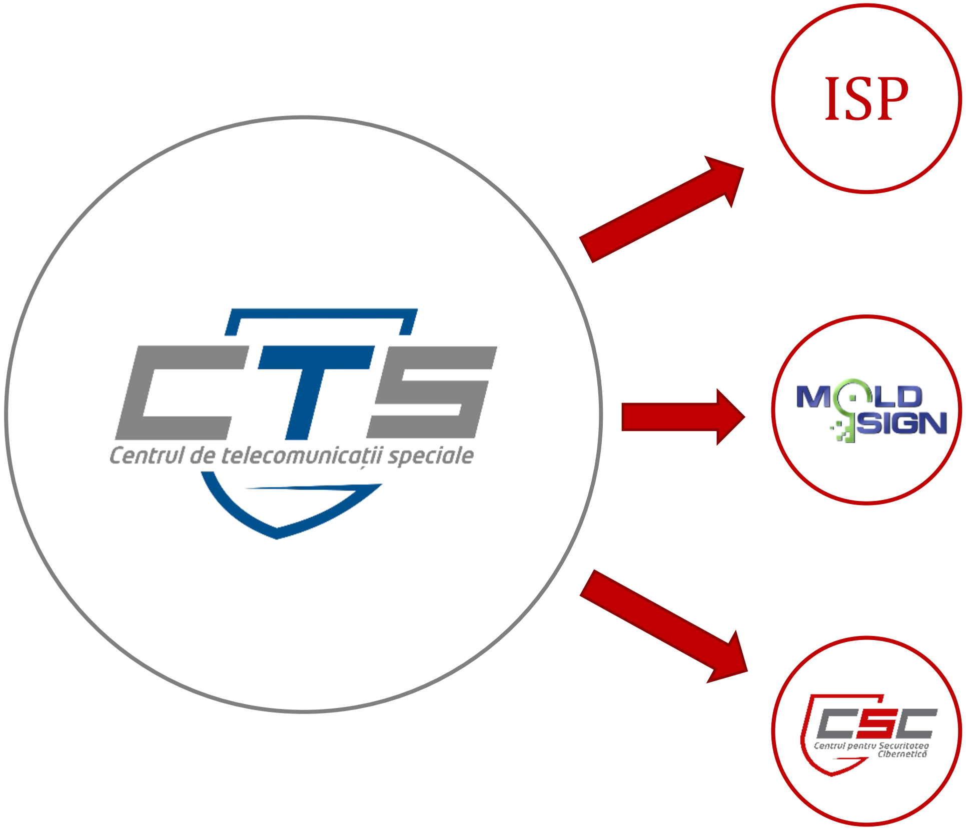
PART I

ABOUT US

CSC

Centrul pentru Securitatea Cibernetică

STATE ENTERPRISE “CENTER FOR SPECIAL TELECOMMUNICATIONS”


CTS
Centrul de telecomunicații speciale
ISP
MOLD SIGN
CSC
Centrul pentru Securitatea Cibernetică

Governmental intranet and Internet provider

- Provides secure communications between government institutions, including transmission of data, voice, email and other services.
- Is a technical operator of governmental cloud M-Cloud platform.

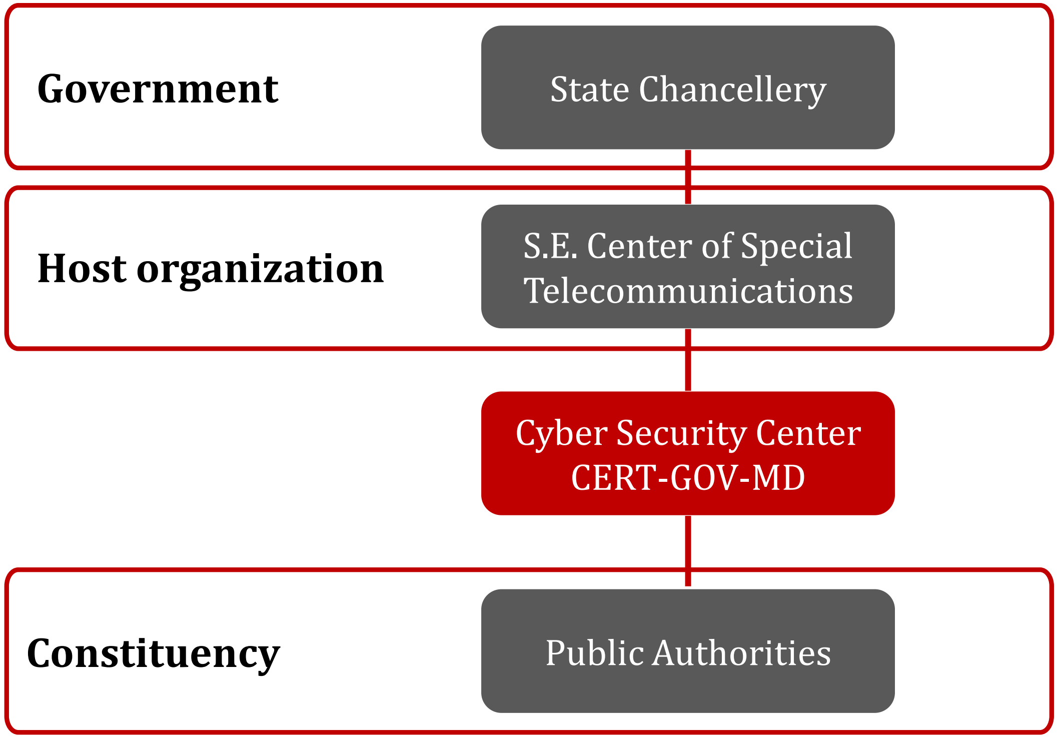
Public Key Infrastructure Provider

- Center issues digital signatures with legal force and authentication certificates.
- In 2014 center provided it services for more than 800 Moldavian companies both public institutions and private sector.

Governmental Cyber Security Center:

- Established in 2010 according to the Government Decision nr. 746 of 18.08.2010 “On the approval of Updated Individual Action Plan of partnership Republic of Moldova – NATO”;
- CERT-GOV-MD's constituency are public authorities of the Republic of Moldova.

ABOUT CERT-GOV-MD



Government

State Chancellery

Host organization

S.E. Center of Special Telecommunications

Cyber Security Center CERT-GOV-MD

Constituency

Public Authorities

- CERT-GOV-MD is a governmental computer security incident response team founded within State Enterprise “Center of Special Telecommunications”.
- CERT-GOV-MD's constituency are public authorities and critical information infrastructure providers of the Republic of Moldova.

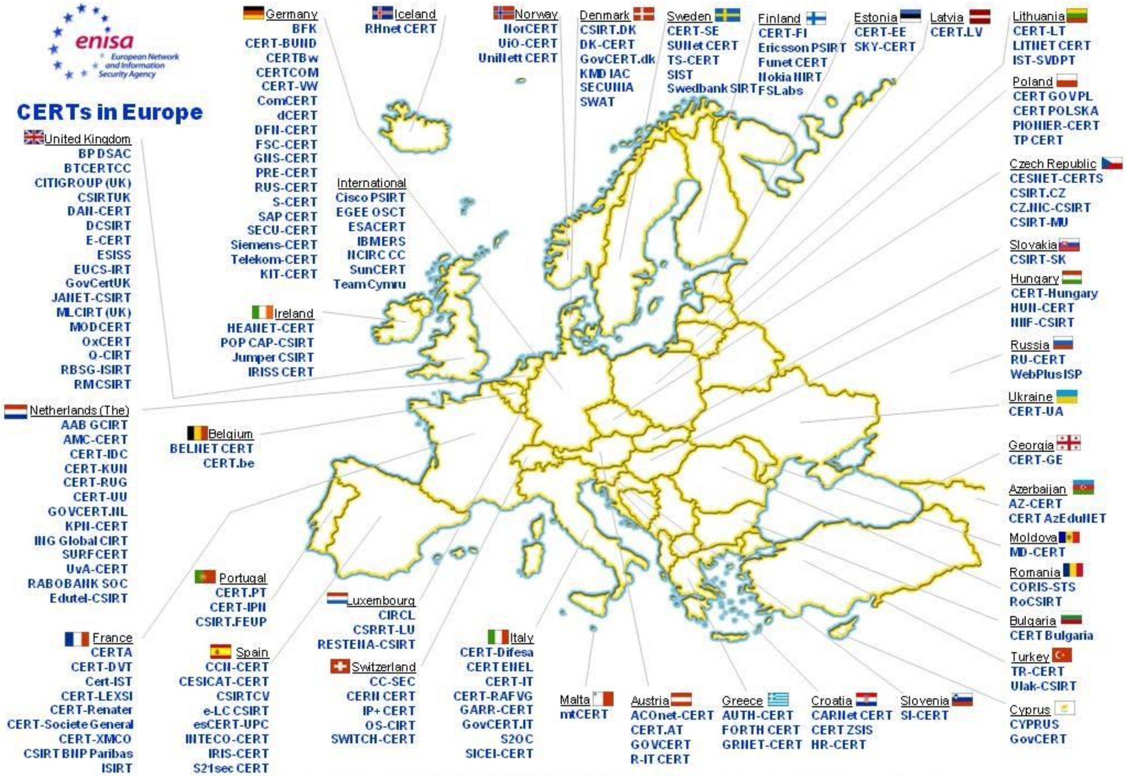
MISSION STATEMENT

“Enhance the capability of the Public Administration Authorities to prepare for and respond to vulnerabilities, threats, and information security incidents in order to protect information and ICT infrastructure.”

CERT-GOV-MD FUNCTIONS

- Providing information about incidents
- Giving support in handling incidents
- Coordinating the response to large-scale incidents
- Sharing data and knowledge

INTERNATIONAL COOPERATION



CERTS in Europe map, February 2011 v2.3 http://www.enisa.europa.eu/act/cert/background/inv © European Network and Information Security Agency (ENISA)

ENISA – CERTs in Europe

January 13, 2014

CERT-GOV-MD is accredited by Trusted Introducer

Benefits:

- Early access to sensitive information regarding ongoing attacks and vulnerabilities detected;
- A secure communication channel between trusted members.

INTERNATIONAL COOPERATION

EXPERTISE FRANCE

CIVIPOL CONSEIL

IMPACT
INTERNATIONAL MULTILATERAL PARTNERSHIP AGAINST CYBER THREATS

Enhancing Cyber Security Project

CENTRUL NAȚIONAL DE RĂSPUNS LA INCIDENTE DE SECURITATE CIBERNETICĂ
CERT-RO

CERT.GOV.GE

shadowserver

enisa
European Network and Information Security Agency

KASPERSKY lab

Bitdefender

TEAM CYMRU COMMUNITY SERVICES

NATO OTAN

PART II

BUILDING AN EFFECTIVE NATIONAL CSIRT

WHAT IS A NATIONAL CSIRT?

A CSIRT – is an organization or capability that provides services and support, to a defined constituency, for preventing, handling and responding to computer security incidents.

A National CSIRT – is a CSIRT which has responsibility for a country or economy.

WHY CREATE A NATIONAL CSIRT?

The focus of a national CSIRT, from a cyber perspective, is to protect:

- national and economic security;
- the ongoing operations of a government;
- the ability of critical infrastructures to continue to function.

A national CSIRT:

- monitors incidents at a national level;
- identifies incidents that could affect critical infrastructures, defense, and the economy;
- warns critical stakeholders and the nation about computer security threats;
- helps build organizational CSIRTs in the public and private sectors.

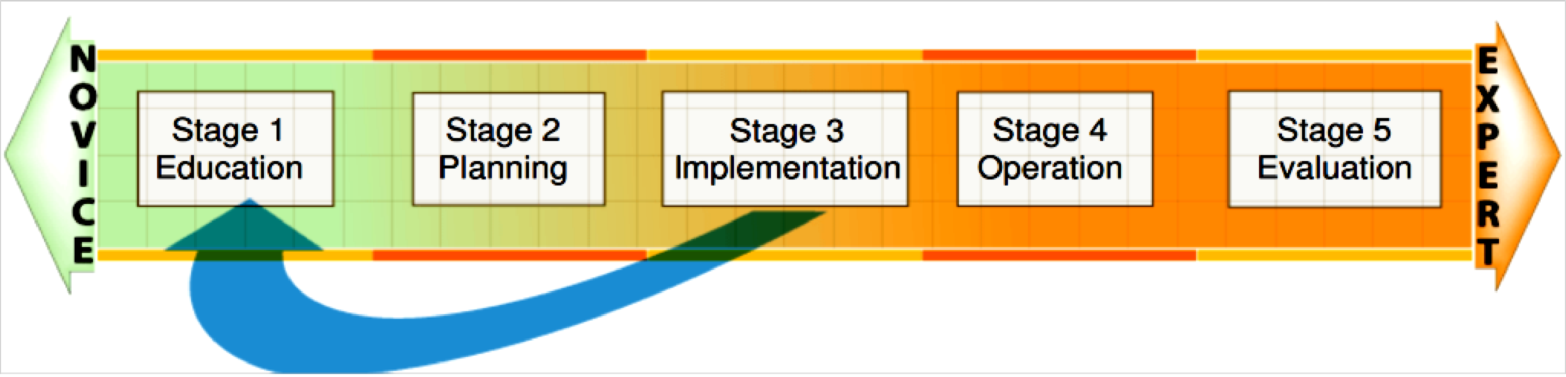
STARTING POINTS

Keep in mind that:

- All CSIRTs are different;
- There is no an universal procedure which will fit for the purposes of establishing a particular National CSIRT.

STAGES OF CSIRT DEVELOPMENT

- **Stage 1** – Education the organization;
- **Stage 2** – Planning the CSIRT;
- **Stage 3** – Implementing the CSIRT;
- **Stage 4** – Operating the CSIRT;
- **Stage 5** – Continuous evaluation and improvement.



STAGES OF CSIRT DEVELOPMENT.
STAGE 1 - EDUCATION THE ORGANIZATION

Understand the environment a national CSIRT will operate:

- Understand what is behind the need of creation of a national team. (what has to be protected? from what? under which regulatory requirements?);
- Understand what are developing capacities (available resources, infrastructure, funding sources, possible partnerships);
- Determine the specific laws, regulation and other policies that will affect the national CSIRT development (compliance issues, level of authority, constraints).
- Understand the potential set of core services that a national CSIRT may provide to its constituency.

STAGES OF CSIRT DEVELOPMENT.
STAGE 2 - PLANNING THE CSIRT

Prepare a national CSIRT concept and obtain funding:

- Outline the requirements for national CSIRT (Take into account: regulatory and law requirements, types of services, level of services);
- Develop a vision for how the national CSIRT will operate (define CSIRT's mission, constituency, services, communication interfaces, organizational model, processes, authority, physical location; determine equipment, infrastructure and staff requirements).
- Develop implementation plan;
- Obtain sponsorship and support (national or governmental approval)

STAGES OF CSIRT DEVELOPMENT.
STAGE 3 - IMPLEMENTING THE CSIRT

Build and implement the national CSIRT:

- Implement secure information systems and network infrastructure to operate the national CSIRT;
- Develop operational policies and procedures for the CSIRT staff.
- Identify and hire personnel, perform appropriate staff training and education.
- Establish points of contact with your constituency as well as communication mechanisms;
- Announce broadly that a national CSIRT is being created and where additional information can be obtained.

STAGES OF CSIRT DEVELOPMENT. STAGE 4 - OPERATING THE CSIRT

Operate the national CSIRT:

- Actively provide services to the constituency;
- Participate in data and information sharing activities and supporting the development of standards for data and information sharing between partners, other CSIRTs and constituents
- Promote the development of organizational CSIRTs within the nation’s constituency and serving as a role model in the development of best practices for these newly developing CSIRTs.
- Develop and implement a mechanism for evaluating the effectiveness of the national CSIRT operations.

STAGES OF CSIRT DEVELOPMENT.
STAGE 5 – CONTINUOUS EVALUATION AND IMPROVEMENT

Continuously evaluate and improve the national CSIRT:

- Track any changes in the constituency, legislation, policy or other regulations that will affect the overall mission and goals of the national team;
- Improve the national CSIRT according to the results of evaluations;
- Continue to develop and enhance CSIRT policies and procedures;
- Improve the quality of CSIRT activities by providing training, workshops, conferences that discuss attack trends and response strategies.

REFERENCE MATERIALS

- **CERT® Program's Resource for National CSIRTs**

  http://www.cert.org/csirts/national/
- **CERT listing of National CSIRTs**

  http://www.cert.org/csirts/national/contact.html
- **Staffing Your Computer Security Incident Response Team – What Basic Skills Are Needed?**

  http://www.cert.org/csirts/csirt-staffing.html
- **Resources for Computer Security Incident Response Teams (CSIRTs)**

  http://www.cert.org/csirts/resources.html
- **Defining Incident Management Processes: A Work in Process**

  http://www.cert.org/archive/pdf/04tr015.pdf
- **ENISA: Support for CERTs / CSIRTs**

  http://www.enisa.europa.eu/act/cert/support
- **ENISA: Baseline capabilities for National CSIRTs**

  http://www.enisa.europa.eu/act/cert/support/baseline-capabilities

THANK YOU FOR ATTENTION!

QUESTIONS?

Centrul pentru Securitatea Cibernetică

Cyber Security Center CERT-GOV-MD, S.E. CTS

www.cert.gov.md

Follow us on Facebook!
www.facebook.com/CERTGOVMD

Incident report
info@cert.gov.md
Tel. +373 22 820 900