WWW.CERT.RO

CENTRUL NATIONAL DE RASPUNS LA INCIDENTE DE SECURITATE CIBERNETICA
ROMANIAN NATIONAL COMPUTER SECURITY INCIDENT RESPONSE TEAM

CERT-RO – short summary

Established by Government Decision no. 494/2011

Nationwide incident response

Romanian national cyberspace

Independent structure

Prevent
Analyze
Identify
Respond

Key activities

CERT-RO

Awareness Campaigns

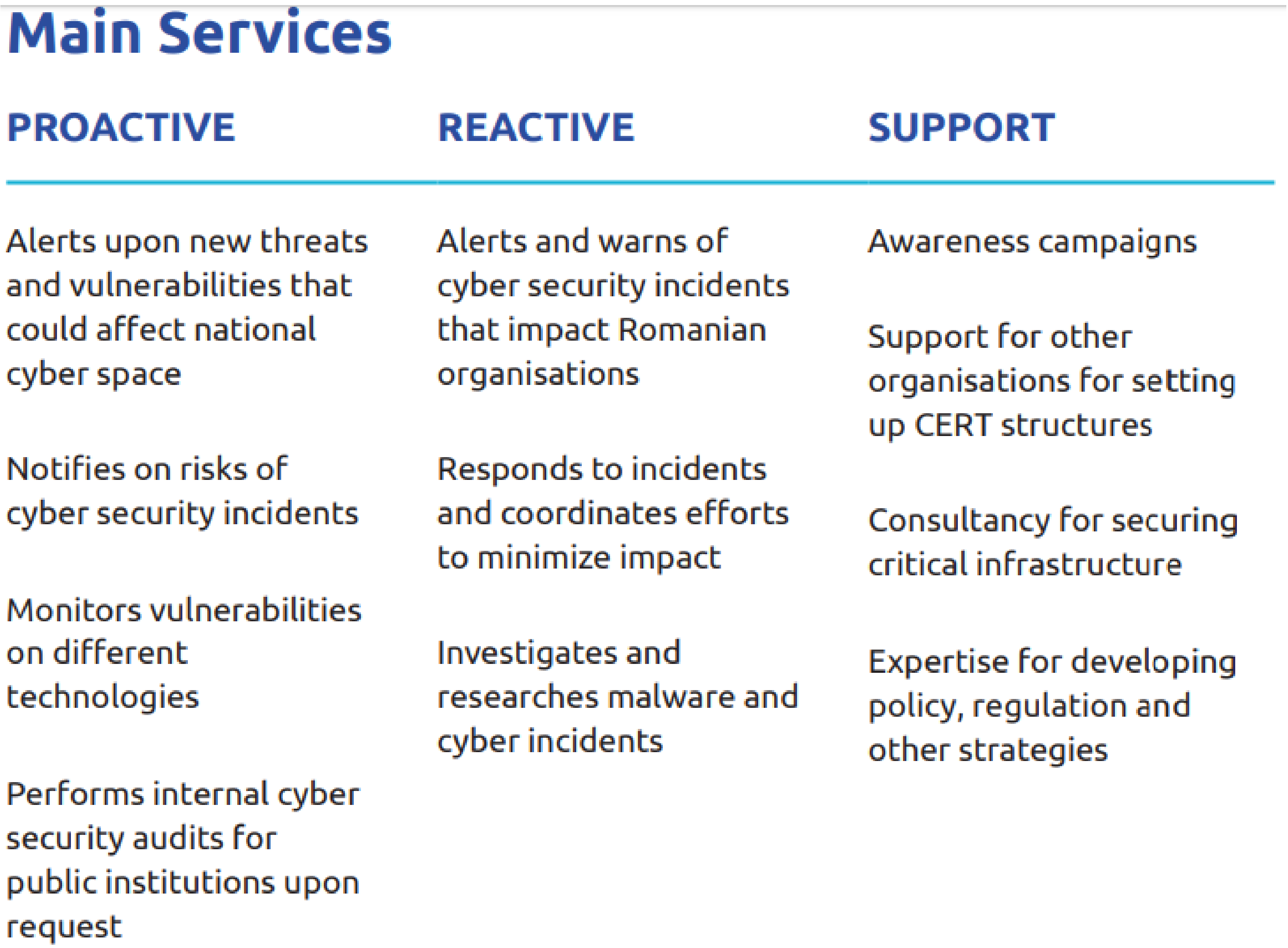
National Point of Contact

Security Audits

Early Warning System

Incident Response Activities

Our work



Main Services

PROACTIVE

Alerts upon new threats and vulnerabilities that could affect national cyber space

Notifies on risks of cyber security incidents

Monitors vulnerabilities on different technologies

Performs internal cyber security audits for public institutions upon request

REACTIVE

Alerts and warns of cyber security incidents that impact Romanian organisations

Responds to incidents and coordinates efforts to minimize impact

Investigates and researches malware and cyber incidents

SUPPORT

Awareness campaigns

Support for other organisations for setting up CERT structures

Consultancy for securing critical infrastructure

Expertise for developing policy, regulation and other strategies

Legal grounds & Regulations

National Legislative Acts concerning the cyber security area:

Government Decision no. 494/2011 for the establishment of CERT-RO - computer security incident response team, a specialized organization responsible for preventing, analyzing, identifying and reacting to cyber incidents in Romania.

Government Decision no. 271/2013 for the approval of the Romanian National Cyber Security Strategy and National Action Plan for the implementation of the National Cyber Security System

Legal grounds & Regulations

Government Decisionno.245, from April 7th 2015, for the approval of the National Strategy regarding the Digital Agenda for Romania 2020

NIS Directive, from August 2016, Directive of the European Parliament and of the Council concerning measures for a high common level of security of **network and information systems** across the Union

Romanian Cyber Security Strategy (1)

- **GD271/2013**
- Establishes the objectives, principles and major directions of action in prevention and response to threats, vulnerabilities and risks to the Romanian cyberspace.
- Establishes the National Cyber Security System (SNSC)
  - a cooperation framework at national level
  - consists of public authorities and institutions with responsibilities and capabilities on cyber security.
  - defines also cooperation with academia, private entities, associations and NGOs

Romanian Cyber Security Strategy (2)

- Establishes the Operative Council on Cyber Security (COSC) as the coordination body consisting of representatives from ministries and other national institutions and competent authorities.

- **Oct 2017** - Ministry of Communications launched in public consultation a law proposal for transposing the NIS directive.

Romanian Cyber Security Strategy (3)

- **May 2018** - Law was approved by the Parliament (end May 2018)
- **July 2018** – The law was contested at Constitutional Court
- **November 2018** – NIS Directive is in the process of approval once again in the Romanian Parliament.
- Reached the decisional chamber.

Challenges

- Lack of any law enforcement capabilities
- Users being misinformed regarding our role
- Weak digital skills of the population
- Poor cyber security education of the common user

Internet Usage Statistics

11 million Internet Users in **Romania** (2017)

Share of Romania Population: **58 %** (penetration)

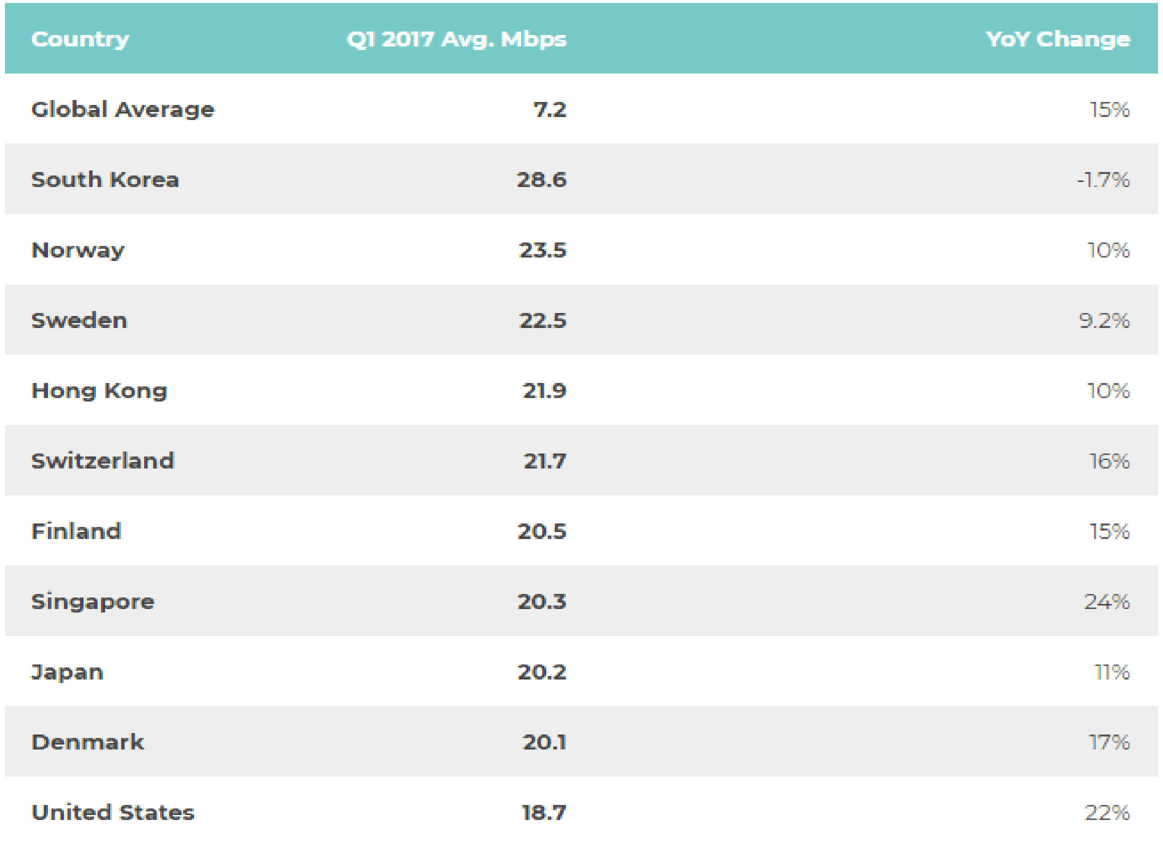
Total Population : **19.71 million**

Share of World Internet Users: **0.3 %**

Internet Users in the World: ~ **3.8 billion**

Sources:

http://www.internetlivestats.com/, Romanian National Statistics Institute



Country	Q1 2017 Avg. Mbps	YoY Change
Global Average	7.2	15%
South Korea	28.6	-1.7%
Norway	23.5	10%
Sweden	22.5	9.2%
Hong Kong	21.9	10%
Switzerland	21.7	16%
Finland	20.5	15%
Singapore	20.3	24%
Japan	20.2	11%
Denmark	20.1	17%
United States	18.7	22%

Source

Fastmetrics.com

Statistics from 2017

- **33,71%** of the total number of unique IPs from RO were involved in at least one cyber security alert processed by CERT-RO in 2017
- **83,63%** of the processed alerts account for vulnerable IT systems
- **10,32%** of alerts are addressing compromised IT systems
- **5,88%** (8,17 mil.) of alerts regarding IT systems infected with Botnet
- **1709 .ro web domains** were reported by CERT-RO as being **compromised**, 84% less than in 2016.

CERT-RO

ROMÂNIA

1918-2018 | SĂRBĂTORIM ÎMPREUNĂ

Evolution of the Cyber Threat Landscape 2017

CERT-RO eCSI project

- ”Enhanced National Cyber Security Services and Capabilities for Interoperability – eCSI”
- Financing source: CEF Telecom program

  CEF–TC–2016–Call 3: Cyber Security
- Financing: INEA - Innovation and Networks Executive Agency
- EU contribution: 869.000 EURO (75% of total eligible expenses)
- Implementation period: 24 months (01.09.2017- 30.08.2019)

SCOPE of eCSI project

- Create, maintain and expand the cybersecurity capabilities of CERT-RO.

- Extending the cyber security services we provide at national level;

- Reach a state of preparedness that will allow us to participate on equal footing at European level.

eCSI project – specific objectives

- Expand the cybersecurity services provided by CERT-RO

- Interconnect CERT-RO and other national cybersecurity capabilities and services with MeliCERTes, facilitating an efficient information sharing and cyber incidents management

- Ensure the compliance with the requirements set out by the NIS Directive.

- Build awareness about technical and organizational requirements for achieving a good level of cybersecurity.

eCSI project – activities

- **NCSP – National Cybersecurity Services Platform**
- **National Cyber Call Centre (NC3)**
- **Digital Forensics and Malware Analysis Laboratory**
- **Joint Cybersecurity Trainings**
- **Dissemination, Cooperation and Sustainability**

National Cybersecurity Services Platform

CERT-RO

- technical platform consisting of hardware and software which will increase CERT-RO's technical capabilities related to cybersecurity incident management and information sharing;
- interoperable with the EU cooperation mechanisms and the Cybersecurity Core Service Platform (CSP)
- collect, process, disseminate and share data related to cybersecurity incidents, vulnerabilities, threats, events and artefacts, including incident notifications received by CERT-RO
- platform will provide services for different national organizations: digital service providers and operators of essential services (as defined by the NIS Directive), Internet Service Providers, law enforcement authorities, national cybersecurity authorities and other organizations within CERT-RO constituency.

National Cyber Call Centre (NC3)

- Enhancing the communication infrastructure by adding a National Cyber Call Centre.
- Available 24/7 for all citizens, as well as public or private organizations.
- With NC3, CERT-RO will meet the requirements imposed to national CSIRTs by the NIS Directive: set-up of several means for being contacted and for contacting others at all times.

Digital Forensics & Malware Analysis Laboratory

- Dedicated laboratory equipped with specialized toolkits and a sandbox platform for automation of malware analysis tasks will be set up;

- CERT-RO personnel responsible for Digital Forensics and malware analysis activities will be trained to acquire more specific expertise in these areas

The fantasy is as real as the reality.

Awareness campaigns for all types of users

312	0	12	16
DAYS	HOURS	MINUTES	SECONDS

October is CyberSecMonth

1st – 31st October 2018

CERT-RO

THANK YOU!

MIHAI ROTARIU

P: +40740066866

E: mihai.rotariu@cert.ro