Romanian National Computer Security Incident Response Team
CERT-RO

dan.tofan@cert-ro.eu
http://www.cert-ro.eu
About

• A Digital Agenda for Europe, Pillar : Trust and Security, Action 38
  – Member States to establish pan-European Computer Emergency Response Teams: Member States should establish by 2012 a well-functioning network of CERTs at national level covering all of Europe.

• G.D. 494 / 2011 establishes CERT-RO, starting from 11.05.2011:
  – Prevent, analyze, identify and respond to cyber security incidents related to Romanian cyber-space.
  – National contact point, regarding cyber-security incidents, with similar structures within or outside Romania.
  – Develops national IT security policies and strategies along with other Romanian public authorities and proposes regulations regarding national cyber-security strategy.
  – Official advisor of the national public authorities, regarding critical infrastructure cyber-protection.
Organizational chart

- General Director
- Deputy Director
  - Technical Department (9 persons)
  - Legal & Policies Department.
  - Cooperation & Dissemination Department (public relations).
  - Economic & Financial Department.
Coordination Comitee

Formed by reprezentants of:

– Ministry of Communication and Information Society;
– Ministry of National Defence;
– Ministry of Administration and Interior;
– Romanian Intelligence Service;
– Foreign Intelligence Service;
– Special Telecommunications Service;
– Protection and Guard Service;
– National Registry Office for Classified Information;
– National Authority for Management and Regulations in Communications
National Partners

• **CERT-RO Community in România**
  – CERT entities within public or private institutions/companies in Romania.
    • CorisSTS
    • RoCSIRT
    • CertMil
  – Institutions within our Coordination Comitee.
  – Some private companies: ISP, security solutions providers etc.

• **Future projects**: better cooperation with the private sector.
International partners

- European Network and Information Security Agency (ENISA).
- TRUSTED INTRODUCTER – TERENA TF-CSIRT – status CERT-RO “accredited member” since 09.03.2012.
- Other CERTs from TI.

- **Future objectives**: FIRST accreditation (Forum of Incident Response and Security Teams) and EGC application.
## Services

<table>
<thead>
<tr>
<th>Proactive</th>
<th>Reactive</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Cyber-security warnings and announcements</td>
<td>• Cyber-security alerts.</td>
<td>• Training other CERT teams and security response teams.</td>
</tr>
<tr>
<td>• Cyber security audits and vulnerability assessments</td>
<td>• Incident coordination and response.</td>
<td>• Security awareness building (events, conferences, courses etc.).</td>
</tr>
<tr>
<td>• Cyber-security application development</td>
<td>• Incident analysis &amp; investigation.</td>
<td></td>
</tr>
<tr>
<td>• Security related information and dissemination</td>
<td>• Incident management at national level.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Incidents

• **Automatic response:**
  – We receive a lot of incidents from partners and the majority of them are processed automatically.

• **Manual response:**
  – Infected websites: 10
  – Hacking against some public institutions in Romania: 7
  – DoS: 5
  – BotNet: 2
Projects

• National Early Warning System
• Cyber-security Web Portal
• Cyber-Security Training Center
• Workgroups regarding national legislation and regulations:
  – Public online services security standards.
National EWS

- **Scope**: Real-time warnings and reports regarding the spreading and the nature of cyber attacks. It will be developed in cooperation with other Romanian organizations, in order to prevent and respond to cyber attacks.

- **Participants**:
  - national authorities that deal with cybercrime in Romania.
  - public institutions.
  - private companies that own or manage cyber infrastructures that are of public utility (ISPs).
  - Any other interested organization.
alerts@cert-ro.eu

- Single contact point for security incidents.

office@cert-ro.eu

- For any other stuff

www.cert-ro.eu

- Web portal with alerts, news, events and security guides.
Thank you!
Questions!