What is a CERT (CSIRT)?

A Computer Security Incident Response Team (CSIRT) is a service organization that is responsible for receiving, reviewing, and responding to computer security incident reports and activity. Their services are usually performed for a defined constituency that could be a parent entity such as a corporation, governmental, or educational organization; a region or country; a research network; or a paid client.”

(CERT/CC)
What is a CSIRT?

- Team within an organisation that prevents, manages and responds to information security incidents
  - Nominated person(s), typically in smaller organisations
  - Specialist team
- Defined contact point – internally and externally
- Historically responsive, CSIRTs increasingly focus on:
  - Prevention and Detection
  - Alerting
  - Vulnerability Analysis
  - Development of business continuity plans
  - Coordination with other CSIRTs
## Recognised CSIRTs in ENOG region

<table>
<thead>
<tr>
<th>Country</th>
<th>CSIRT</th>
<th>Type</th>
<th>TI Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Armenia</td>
<td>CERT-AM</td>
<td>National?</td>
<td>Accredited</td>
</tr>
<tr>
<td>Azerbaijan</td>
<td>AzScienceCERT</td>
<td>R&amp;E</td>
<td>Accredited</td>
</tr>
<tr>
<td></td>
<td>CERT.AZ</td>
<td>National?</td>
<td>Accredited</td>
</tr>
<tr>
<td></td>
<td>CERT.GOV.AZ</td>
<td>Government</td>
<td>Accredited</td>
</tr>
<tr>
<td>Georgia</td>
<td>CERT-GE</td>
<td>R&amp;E</td>
<td>Listed</td>
</tr>
<tr>
<td></td>
<td>CERT-GOV-GE</td>
<td>Government</td>
<td>Accredited</td>
</tr>
<tr>
<td>Kazakhstan</td>
<td>KAZRENA-CERT</td>
<td>R&amp;E</td>
<td>Listed</td>
</tr>
<tr>
<td></td>
<td>KZ-CERT</td>
<td>Government</td>
<td>Listed</td>
</tr>
<tr>
<td>Moldova</td>
<td>CERT-GOV-MD</td>
<td>Government</td>
<td>Accredited</td>
</tr>
<tr>
<td></td>
<td>MD-CERT</td>
<td>R&amp;E</td>
<td>Listed</td>
</tr>
<tr>
<td>Russia</td>
<td>CERT-GIB</td>
<td>ccTLD</td>
<td>Accredited</td>
</tr>
<tr>
<td></td>
<td>Gov-CERT.RU</td>
<td>Government</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>RU-CERT</td>
<td>National?</td>
<td>Accredited</td>
</tr>
<tr>
<td></td>
<td>WebPlus ISP</td>
<td>Commercial</td>
<td>Listed</td>
</tr>
<tr>
<td>Uzbekistan</td>
<td>UZ-CERT</td>
<td>Government</td>
<td>-</td>
</tr>
<tr>
<td>Kyrgyzstan</td>
<td>None?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tajikistan</td>
<td>None?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Turkmenistan</td>
<td>None?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Why are CSIRTs important?

- Security threats are real and ongoing
- Ignoring threats costs resources
  - Denial-of-Service
  - Data Theft
  - Compromises reputations
- Prevention is better than cure
- Small things often prevent disasters
- End user awareness reduces problems
- CSIRTs save more than they cost, and offer possibility to offer value-added services
Why the need for National CSIRTs?

- CSIRTs usually serve particular constituencies (e.g. government, academic, private sector)
- Many security incidents are cross-constituency and international
  - Need for official national points of contact
  - Need for national focal point within country to coordinate incidents
- Operational requirements for national constituencies can be different to other constituencies (e.g. 24 x 7 is more likely needed)
- Key elements of Critical Infrastructure Protection
Why the need for National CSIRTs?

- Internet has become critical to national economies
  - Share knowledge, resources and tools
  - Compare working practices
  - Develop common best practices and standards
  - Encourage development of CSIRTs and/or organisational points of contact.

- Improve coordination with law enforcement, security and military agencies

- Provision of technical advice on cybersecurity to policy makers.

- EU called on all member states to establish National CSIRTs by 2011.
Different models for National CSIRTs

- **Host organisation**
  - National Telecommunications Regulatory Body
  - Government CSIRT
  - Academic CSIRT (often these are the first CSIRTs established in a country)
  - Establishment of National Cybersecurity Centre

- **Voluntary vs Regulated**
  - Relies on willingness of constituents to cooperate, or constituents are required to implement measures to counter threats (only in emergency situations?)

- **Cooperation**
  - Bi/multi-lateral or Community
Examples of National CSIRTs

- **CERT-GOV-MD (Moldova)**
  - Operated by State Center for Special Telecommunications, provider of secure communications between government institutions

- **NCSC-NL (Netherlands)**
  - Operated by Ministry of Security and Justice

- **NorCERT (Norway)**
  - Operated by National Security Authority (NSM), under the Ministry of Defence

- **CERT.be (Belgium)**
  - Operated by BELNET, the National Research & Education Network
How to establish a CSIRT?

- Define basic framework
  - Mission Statement (what to do?)
  - Definition of Constituency (for whom?)
  - Relationship with others (who to cooperate with, and whom to trust?)
- Establish policies
- Determine what services to offer
- Train staff
- Establish incident handling system
- Raise awareness of CSIRT in your community
- Establish contacts with other teams
Types of CSIRT services

- **Reactive**
  - Vulnerability handling alerts
  - Incident & artefacts handling

- **Proactive**
  - Announcements & information dissemination
  - Security audits
  - Development of security tools
  - Configuration & maintenance
  - Intrusion detection

- **Security Quality**
  - Risk analysis
  - Disaster recovery planning
  - Consulting
  - Education
  - Product evaluation
The need to allocate resources to a CSIRT

- Handling security is a service activity
- Incidents require timely and effective response
- Roles and responsibilities are important
- A formal CSIRT structure is a requirement to join the Security Community and benefit from it
- There must be somebody handling a security problem, whose priority is to solve the problem, or at least to take effective countermeasures
- Establishing a minimal Service Level requires a minimal allocation of resources
- Some incidents cannot be handled “best effort style”
The benefits of allocating resources to a CSIRT

- Roles are defined, procedures are established
- People know what to do and how
- Increase in confidence by the community towards the CSIRT
- Increase in confidence by the community towards the host organisation
- Money costing resources (network infrastructure, data, computer services, manpower) are preserved and protected
- Better reputation means better collaboration
The requirements for an operational CSIRT

- Provide and keep updated information about itself and its services
  - Trusted Introducer Listing

- Accomplish a list of operational requirements
  - MUST, SHOULD, MAY lists

- Having operational tools that can solve/neutralize/mitigate security incidents

- Belong to the Web-of-Trust of Security Teams
  - Trusted Introducer Accreditation process
  - FIRST membership
MUST...

- Provide and make available PGP team and members keys
- Provide and keep up-to-date Web site with contact information
- Acknowledge incoming incidents and issue Trouble Tickets or Unique Identifiers
- Inform external teams of unexpected security related discovered information
- Provide incident closure information to the team who opened it
- Use encryption to protect sensitive or personal data in incident handling information exchange
- Keep all incident information confidential and not disclosed beyond the scope of incident handling
- Sign all e-communications with PGP keys
SHOULD...

- Document and publish Best Common Practices (BCP)
- Make available its Communication and Authentication Policy for keys and certificates
- Acknowledge incoming incident handling requests, and state its own Severity classification
- Inform the external team about progress in handling incidents
- Use a Trouble Ticket System (or equivalent) in handling procedures
- Have PGP keys countersigned by other teams
- Install and use security tools
MAY...

- Inform the external team who opened an incident about the internal escalation procedures used
- Redirect the external team who opened an incident to a more appropriate Security Team
- Include automated information (IODEF-like) in reports exchanged with other teams
- Make available X.509 team and members certificates to other teams, including information about the Issuing Certification Authority, in case of Self Signed CA
Trusted Introducer

- CSIRTs rely on notion of trust – whether contacts are trustworthy
- Trusted Introducer service was introduced to establish higher level of trust
- CSIRTs must provide specific information about personnel and services
- Prospective CSIRTs must have support of at least two other TI-accredited CSIRTs, and others can object to acceptance
- Accredited CSIRTs are contacted 3 times per year, and must respond to maintain accreditation
- TI service is operated by TF-CSIRT, the European Forum of Computer Incident Response Teams, but open to all teams
TRANSITS Training

- TF-CSIRT has produced training material for CSIRTs seeking relevant training
- TRANSITS-I is 2-day basic course covering organisational, technical operational and legal issues
- TRANSITS-II is 3-day advanced course covering traffic flow analysis, forensics, communication and incident handling exercises
- Usually 2 x TRANSITS-I and 1 x TRANSITS-II workshop per year in Europe/Mediterranean/Middle East
- TRANSITS materials adopted by FIRST who run workshops elsewhere in the world, and other organisations may also use materials under licence for their own training events
- TRANSITS trainers can be hired for dedicated workshops
Thank You!

Kevin Meynell
meynell@isoc.org