CERT operational gaps and overlaps

ENISA’s report - December 2011


Dufkova Andrea; ENISA, CERT-relations
My goal for today is to...

Meet you...greet you....chat with you!

In addition

• Introduce an interesting report for and from our community
• Discuss with you the findings and recommendations
• Continue receiving your feedback concerning ENISA’s future activities in the CERT area...

• ...and, of course, drink a coffee (beer) with you!
WP2011 > WS1 > WPK 1.4 > Analysis of operational gaps and overlaps on European level

Under its mandate ENISA has been tasked with analysing how CERT cooperation can be further facilitated on a European level, by examining operational needs and whether overlaps exist.

★ Analysis of key operational activities that the national / governmental CERTs carry out

★ Focus on main services:
  ★ Incident Handling
  ★ Alerts & Warnings
  ★ Malware analysis (Artifact handling)
  ★ other

★ Suggestions for ENISA how to further complement and facilitate these activities
CERT operational gaps and overlaps report

Methodology

- Desktop research – on operational activities that the n/g CERTs in Europe carry out to support their constituency...
  
  (the survey aimed to determine which services are most commonly provided and where the CERTs themselves see the most opportunities for reducing overlaps and opportunities where ENISA could possibly support them. The survey also gave participants the opportunity to enter their personal views in open comment fields.)

- Project survey – 20 CERTs responded

- Follow up interviews –...CERT Bulgaria, CERT-BUND, CERT.GOV.PL, Danish GovCERT, IRISS-CERT, mtCERT,...

- Project analysis of all gathered information

- Observations

- Recommendations
Based on the survey responses from the n/g CERTs, the incident handling and alerts & warning services provide the most opportunity for at least some synergies with other CERTs or with central bodies.

- **Incident handling** - recognised as the service which is the most eligible for synergies, incident handling also appears to be the service on which the CERTs cooperate the most;
- **Announcements** - While 15 out of 20 respondents acknowledged the potential for synergies, only half of them actively cooperate on providing this service;
- **Alerts & warnings** - About the same number of respondents believe in the eligibility for cooperation compared to the announcements service, while more respondents are already cooperating;
- The same phenomenon is noticed for **artifact handling**.
...in the operational aspects of the services provided by national/governmental CERTs, in order to complement and facilitate the current operations of the CERTs on a European level.

Two Scoring systems: 1. support by the stakeholders; 2. ENISA mandate support.

- Low acceptance/no mandate support
- Medium acceptance/partial mandate support
- High acceptance/complete mandate support
## Gaps and overlaps – recommendations

<table>
<thead>
<tr>
<th>Observation</th>
<th>Gap or overlap</th>
<th>CERT community acceptance</th>
<th>ENISA mandate support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Harmonisation of legal framework for information sharing and international incident handling</td>
<td>Gap</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Guidance and direction based on observed trends</td>
<td>Gap</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Industry partnerships</td>
<td>Overlap</td>
<td></td>
<td></td>
</tr>
<tr>
<td>European institutions CERT</td>
<td>Gap</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Providing specialised training</td>
<td>Gap</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Closed CERT-community contacts directory</td>
<td>Overlap</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incident classification and reporting standardisation</td>
<td>Gap</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CERT process guidance</td>
<td>Gap</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stimulating and providing means to centrally exchange information on alerts &amp; warnings among CERTs</td>
<td>Gap</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Providing CERT communications channels</td>
<td>Gap</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
CERT operational gaps and overlaps report

Wrap up

- Gathered information / opinion of external parties
  - Different CERTs have very different views / needs
- Suggestions for ENISA how to further complement and facilitate CERT activities
- 17 recommendations for future activities
  - Assessed relevance to the current and proposed ENISA mandate
  - Assessed ‘CERT community acceptance’ level
CERT operational gaps and overlaps report

Impact

- Alignement of future ENISA activities in CERT area with our community needs and expectations

- Improved and more efficient services provided by national / governmental CERTs

Improved IT security in Europe
Contact

Andrea DUFKOVA
Technical Competence Department - CERT relations
European Network and Information Security Agency

Science and Technology Park of Crete (ITE)
P.O. Box 1309
71001 Heraklion - Crete – Greece

Cert-relations@enisa.europa.eu