How to set up a CSIRT in an ITIL driven organization

Christian Proschinger
Raiffeisen Informatik GmbH
- Introduction R-IT CERT
- Idea
- Introduction to ITIL
- Example Vulnerability Management
- Lessons Learned
How to set up a CSIRT in an ITIL driven organization | public

Outside of Europe:
- China
- Südafrika
- Kasachstan

Raiffeisen Informatik Group

27 Locations
3,000 Employees
Turnover 2009: 1.2 Billion Euro
40 years experience

IT Services
- IT Operations
- Outsourcing
- Security Services
- Client Management
- IT & Software Consulting
- Output Services
Security Competences at Raiffeisen Informatik

- **Department Information Security Management**
  - Information Security Management System
  - ISO 27001
  - Focus on Risk Management

- **Department Security Competence Center**
  - Founded 2005
  - Headquarter of Raiffeisen Informatik CERT Austria
  - Penetration Testing

- **Responsible person/team for each Business Service as well as for each Technical Component**
General Situation

- Large scale IT organization have to be standardized and to be compliant
  - IT Infrastructure Library
  - Business process maps
  - ISO 27001
  - COBIT

- CSIRT
  - Customized services for constituency
  - Guidelines
    - helpful but generic
General Situation

- **IT Infrastructure Library**
  - Best practice library
  - De-facto standard

- 76% of organizations align IT Service Management to ITIL*
- Popular processes
  - Incident Management
  - Service Desk
  - Incident Management Process
  - Problem Management
  - Information Security Management

*IT Service Management Studie MATERNA
Questions

- What are the implications of ITIL concerning
  - setting up a CSIRT
  - operate a CSIRT
Introduction to IT Infrastructure Library

- 5 Core publications
  - Service strategy
  - Service design
  - Service transition
  - Service operation
  - Continual service improvement

- Target is an IT alignment to business processes

Source: ITIL v3 The official Introduction to the Service Lifecycle: TSO (OGC); 2007
How to set up a CSIRT in an ITIL driven organization | public
Example Vulnerability Management

- Information Security Management Process
  - ISO 27001:2005
  - Deming Cycle (Plan-Do-Check-Act)
- CSIRT can produce added value
  - Economies of scale
  - Quality
Example Vulnerability Management

- Vulnerability Management ≠ Patch Management ➞ TRUE
  - Workarounds
  - Configuration issues
  - Design issues
  - Functional patches
Example Vulnerability Management

**PLAN**

- **Information**
  - Input
    - Penetration Tests – CSIRT Service triggered by Information Security Management
    - Security Advisories – CSIRT Service
    - Service Desk

**DO**

- **Countermeasure**
  - Problem Management
    - Problem Tickets: Penetration Testing measures, Less critical vulnerabilities
  - Incident Management
    - High critical vulnerabilities

**CHECK**

- **Audit**
  - Vulnerability Scanning – CSIRT Service

**ACT**

- **Report**
  - Information Security Management
### Patch Management: affected ITIL Processes

<table>
<thead>
<tr>
<th>Service Strategy</th>
<th>Service Design</th>
<th>Transition</th>
<th>IT Operations</th>
<th>Service Improvement</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial Management</td>
<td>COST CONTROL</td>
<td>Service Level Management: customer relations interface</td>
<td>Planning and Support</td>
<td>Incident Management: patch (critical)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Review of infrastructure requirements</td>
<td>Service Asset and Configuration Mgmt</td>
<td>Problem Management: patch, root problem search</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Continuity Management to minimize impacts</td>
<td>Change Mgmt</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Risk assessment</td>
<td>Release and Deployment Mgmt</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Vulnerability Management process</td>
<td>Service Validation &amp; Testing Evaluation</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Knowledge Mgmt</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Service Reporting</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Service Measurement</td>
</tr>
</tbody>
</table>

- Service Reporting
- Service Measurement
Lessons Learned

- Vulnerability Management != Patch Management
- Incident != Security Incident
- Service Strategy
  - Utility
  - Warranty ➔ USP Constituency

Service Design
- Information Security Management
  - ISO 27001:2005 good preparation for FIRST accreditation (Site Visit)
  - Information Security Management System
  - Define clear "interfaces"
  - Use the experience of your ISM Team
  - Easy way to achieve “separation of duties”

Service Operation
- Incident Management: Service Desk
  - Process can be easily adopted for security incident management
- Problem Management: Good way to implement penetration test measures
Summary

- Considering ITIL offers advantages
- Important processes
  - Incident Management
  - Problem Management
  - Information Security Management
    - ISO 27001:2005 provides a good basis
- Maybe a possibility to set up the process of CSIRTs easier
Thank you for your attention!