From bullet point journal to lessons learned

How to manage coordination and cooperation development in ad-hoc working environment
Agenda

- What we do @ NCSC-FI?
- How we do it?
  » Bullet point journal
- How do we improve it?
  » Lessons learned
Warning!

This presentation is not technical and does not have any technical details!

It is about handling the flow of technical cases
What we do?

NCSC-FI as an operational team
Incidents handled yearly

<table>
<thead>
<tr>
<th>Incident reports per year</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident reports</td>
<td>Over 1000</td>
</tr>
<tr>
<td>Vulnerability coordination</td>
<td>Over 10</td>
</tr>
<tr>
<td><strong>NCSC-FI monitoring systems</strong></td>
<td></td>
</tr>
<tr>
<td>Autoreporter</td>
<td>50 - 410 000</td>
</tr>
<tr>
<td>HAVARO</td>
<td>Over 100</td>
</tr>
</tbody>
</table>
## Publications yearly

<table>
<thead>
<tr>
<th>Category</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Public</strong></td>
<td></td>
</tr>
<tr>
<td>Blog posts</td>
<td>80</td>
</tr>
<tr>
<td>Facebook &amp; Twitter</td>
<td>Over 100</td>
</tr>
<tr>
<td><strong>Distribution lists</strong></td>
<td></td>
</tr>
<tr>
<td>Week reports</td>
<td>52</td>
</tr>
<tr>
<td>Monthly summaries</td>
<td>12</td>
</tr>
<tr>
<td>Daily news letters</td>
<td>360</td>
</tr>
<tr>
<td>Vulnerability letters</td>
<td>99 (from June 2016)</td>
</tr>
<tr>
<td>CIP-messages</td>
<td>238</td>
</tr>
</tbody>
</table>

Information security in 2016

Publication 001/2017 J of the Finnish Communications Regulatory Authority

Viestintävirasto
Finnish Communications Regulatory Authority
1 duty officer /1week
- Incident response 24/7/365
- triage
- News follow up

2 duty officer /1week
- Blog posts
- Aids 1. duty officer

Coordinator/3weeks
- Coordinates significant incidents
- Follows and coordinates situation awareness

3 duty officer /1week
- HAVARO monitoring
"CERT Public announcements" awarded as information security phonemon of the year 2016

13.05.2017 time 13:02
Alert 02/2017
updated 15.05.2017 time 13:29

Active ransomware campaign - install Windows updates immediately

Cases of the WanaCry/Notpetya ransomware have also been detected in Finland. The ransomware signatures vary aggressively in the internal network of an organisation if the security patches for the vulnerabilities the security patches for which are not installed. To protect against this...
Bullet point journal in coordination

How it is done?
Problems and questions

1. Mostly ad-hoc cases
2. Obtained from variety of sources
3. All having different kind of problems
4. Several people handling them
5. With many cooperation parties

1. What is important and to whom?
2. What to follow for longer?
3. What is the overall situation?
4. Where is it going?
5. Did we do it correctly?
What is a bullet point journal?

The System

The Bullet Journal is a customizable and forgiving organization system. It can be your to-do list, sketchbook, notebook, and diary, but most likely, it will be all of the above. It will teach you to do more with less.

Source: www.bulletjournal.com

- From "Big Picture" to "small details"
- Aid with topics and symbols
Cyberweather follows 6 topics

- Espionage
- DDoS
- Malware and Vulnerabilities
- Fraud & Phishing
- Network Functionality
- IoT
### Daily (morning brief)
- New cases
- Topic news
- Vulnerabilities
- IOC's data
- Monitoring systems
- Customer contacts & networks

### Weekly (report)
- Espionage
- DDoS
- Malware and vulnerabilities
- Fraud & Phishing
- Network functionality
- IoT

### Monthly (trends)
- Cyberweather collage
- Update of statistics and trends

### Yearly (year book)
- Summary & Forecast
- Analyze: TOP5 threats and solutions

**Bullet point journal @ NCSC-FI?**

Head of Cooperation and Situation Awareness | Jarna Hartikainen
#cyberweather in May 2017

Worldwide problems from aggressive WannaCry – ransomware

**Espionage**
- Affecting elections worries all over Europe
- ICT-service providers as a spread vector to organizations

**Denial of service**
- Gigabit DDoSes everyday in Finland
- Several notifications of threatening with DDoSes

**Fraud & Phishing**
- Continues bank and Apple ID phishing has become new normal
- Subscription traps common

**Malware and vulnerabilities**
- WannaCry ransomware spread all over world
- Finland suffered few hits

**Functionality of communication services**
- No significant disturbances lately
- Significantly less disturbances than year ago

**IoT**
- Minimum requirements discussed in EU level
- Scanning industrial control systems 2017 revealed unprotected critical devices in network
# NCSC-FI daily week timetable

<table>
<thead>
<tr>
<th></th>
<th>Mon</th>
<th>Tue</th>
<th>Wed</th>
<th>Thu</th>
<th>Fri</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Daily</strong></td>
<td>Morning brief (coordinator)</td>
<td>Morning brief (coordinator)</td>
<td>Morning brief (coordinator)</td>
<td>Morning brief (coordinator)</td>
<td>Shift of duty (1. duty officer)</td>
</tr>
<tr>
<td><strong>Report</strong></td>
<td></td>
<td></td>
<td>Weekly report - AMBER</td>
<td>Weekly report - GREEN</td>
<td></td>
</tr>
<tr>
<td><strong>Work</strong></td>
<td>Group meetings</td>
<td></td>
<td></td>
<td></td>
<td>NCSC-FI meeting</td>
</tr>
</tbody>
</table>

TLP: green
# NCSC-FI weekly month timetable

<table>
<thead>
<tr>
<th>Week</th>
<th>Mon</th>
<th>Tue</th>
<th>Wed</th>
<th>Thu</th>
<th>Fri</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st</td>
<td>DL: Cyberweather material</td>
<td></td>
<td></td>
<td></td>
<td>Update: Cyberweather</td>
</tr>
<tr>
<td>2nd</td>
<td>DL: Sector reports material</td>
<td>Network functionality</td>
<td>DoS</td>
<td></td>
<td>Sector reports</td>
</tr>
<tr>
<td>3rd</td>
<td>Lessons learned</td>
<td>Malware and vulnerabilities</td>
<td></td>
<td>Espionage</td>
<td></td>
</tr>
<tr>
<td>4th</td>
<td></td>
<td>Phishing</td>
<td></td>
<td>IoT</td>
<td></td>
</tr>
</tbody>
</table>
All gathers to a Year Book

Lessons learned

Improving the way of work
What is lessons learned?

http://www.projectmanagers.net/i/top-mistakes-in-project-management/you-will-make-mistakes/
Lessons learned in action

Improvement ideas and feedback brought up by the employees

- Once a month held discussion session
- 2-4 cases picked up brought up by the employees
- What did we do right/wrong?
  - Improvement ideas listed
  - Taken to management
  - Management decides what ideas are taken into actions to improve future way of work
Results of lessons learned 2016

- 22 cases discussed
- In 9 sessions
- We found
  - 75 ideas!
  - Many success stories
Conclusions

- **Simplify** - with simple topics
- **Check points** - for freedom of doing in ad-hoc
- **Learn** - from the mistakes and successes!