Cyber Weather
Situational Awareness Product For Our Non-technical Constituents
Cyber...WHAT?
Situational awareness?

- What our constituents think it is
- What our management thinks it is
- What society thinks it is
- What it really is
The problem

Regardless of our communication efforts, our constituents were demanding better situational awareness.
Requirements for the new situation awareness product

- Language that also non-technical audience can understand
- Periodically updated
- Cover wide variety of cyber security topics
Six focus areas that are updated monthly

- Denial of Service
- Malware & vulnerabilities
- Phishing & scams
- Spying
- Network performance
- Internet of Things
Behind the simple presentation goes a lot of information from different sources

<table>
<thead>
<tr>
<th>Information sources</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ticketing system</td>
<td>Recent cases and incident reports both from private and public sectors</td>
</tr>
<tr>
<td>Information Sharing and Analysis Centres (ISACs)</td>
<td>TLP: RED information from our critical constituents generalized to TLP:WHITE</td>
</tr>
<tr>
<td>National early warning and monitoring system (HAVARO)</td>
<td>Detections based on threat intelligence and IoC's</td>
</tr>
<tr>
<td>Autoreporter</td>
<td>Malicious network traffic detections in Finland</td>
</tr>
<tr>
<td>Open sources</td>
<td>News, social media, public reports</td>
</tr>
</tbody>
</table>
Cyber weather conditions may be calm, worrying or serious

#Cyber Weather 04/2018

Denial-of-service attacks
- In April, the number of attacks reported in Finland was low.
- A service selling denial-of-service attacks was taken down after an international police operation.

Spying
- American hackers launched a counter-attack on Iranian targets.
- Germany accused Russia of a break-in into government systems.
- Methods used by Chinese spies were exposed.

Malware & vulnerabilities
- A serious vulnerability was found in Cisco ASA products that gave attackers access to VPN networks.

Network performance
- There were fewer significant incidents than normally.

Scams & phishing
- Phishing phone calls targeted the user data of Finnish gaming company Veikkaus Oy.
- Several incidents were found in April where hijacked O365 email accounts were used in scamming.
- There was a huge rise in bank credential phishing attempts.

IoT
- Microsoft released the Azure Sphere platform product for secure IoT products.
Cyber weather is delivered widely to all our constituents

- Critical infrastructure providers (CIP)
- Government
- Media
- Publicly via our website
  » Frontpage available also in English
Initial reception

NCSC-FI managers

NCSC-FI Experts

External
After positive external feedback, also the internal attitude has turned positive
Success factors

- Easy-to-follow language
- Monthly updates
- Familiar metaphor
Benefits

- Key trends and events of the cyberspace
- Device for constituents' internal communication
- Source in risk assessments
- NCSC-FI's own presentations
Situational awareness?

What our constituents think it is
What our management thinks it is
What society thinks it is
What it really is
Situational awareness?

Something the target audience is able to understand and use in their daily work