CERT-NL

How are we doing it?
Who are we ?

CERT -NL is the Computer Emergency Response Team of SURFnet, the Internet provider of the Higher Education institutes and many research organizations in the Netherlands. CERT-NL handles all cases of computer security incidents in which a SURFnet customer is involved as a victim or a suspect.

Since 1992
Main goals

• Incident Response 24x7
  – coordination between involved parties

• Education and awareness
  – advisories
  – seminars etc..
Organizational structure

- Steering Group
- Kernel
- Expert Group
- Site Security Contacts
The Kernel

• Currently 9 members, including chair
  – 6 SURFnet employees
    • from all operational departments
    • for 3 of them substantial part of work
  – 3 ‘external’ members
    • experience
    • belonging to the SURFnet constituency
    • voluntary
The Expert Group

- Selected on specific knowledge or experience
- For things the Kernel does not know
- For special projects
In case of an Emergency

- Emergency phone
  - operated 24x7 by the SURFnet Helpdesk
  - strict procedure
  - kernel member on duty can be paged

- Week shifts by kernel members
  - pager and mobile phone
  - licensed to disconnect
Less urgent

• mail
  – handled by kernel member on duty
  – also during non-office hours

• phone/fax/snail
  – office hours only
Case follow-up

- not part of the week shift
- substantial part of work
Tools

• Trouble ticket system
• Internal website
  – working documents, templates, contact lists….
• Mailing list for Site Security Contacts
• External website
  – http://cert-nl.surfnet.nl/
CERT-NL Advisories

<table>
<thead>
<tr>
<th>Year</th>
<th>Advisories</th>
</tr>
</thead>
<tbody>
<tr>
<td>1991</td>
<td>0</td>
</tr>
<tr>
<td>1992</td>
<td>25</td>
</tr>
<tr>
<td>1993</td>
<td>27</td>
</tr>
<tr>
<td>1994</td>
<td>24</td>
</tr>
<tr>
<td>1995</td>
<td>26</td>
</tr>
<tr>
<td>1996</td>
<td>79</td>
</tr>
<tr>
<td>1997</td>
<td>93</td>
</tr>
<tr>
<td>1998</td>
<td>81</td>
</tr>
<tr>
<td>1999</td>
<td>53</td>
</tr>
</tbody>
</table>
CERT-NL Mail

![Bar chart showing the number of CERT-NL Mail from 1991 to 1999.]

- 1991: 1
- 1992: 513
- 1993: 1591
- 1994: 1773
- 1995: 1626
- 1996: 1816
- 1997: 2113
- 1998: 2488
- 1999: 4199
Logged events 1999

- Abusive Comms: 7
- Administrative: 62
- Denial of Service: 22
- LAN Sniffing: 2
- Other: 10
- Probe: 137
- Root Compromise: 19
- Spam Mail: 45
- Trojan: 18
- Unauthorized Use: 11
- Virus: 0
- Warez: 2