

CERT-NL

How are we doing it ?

Who are we ?

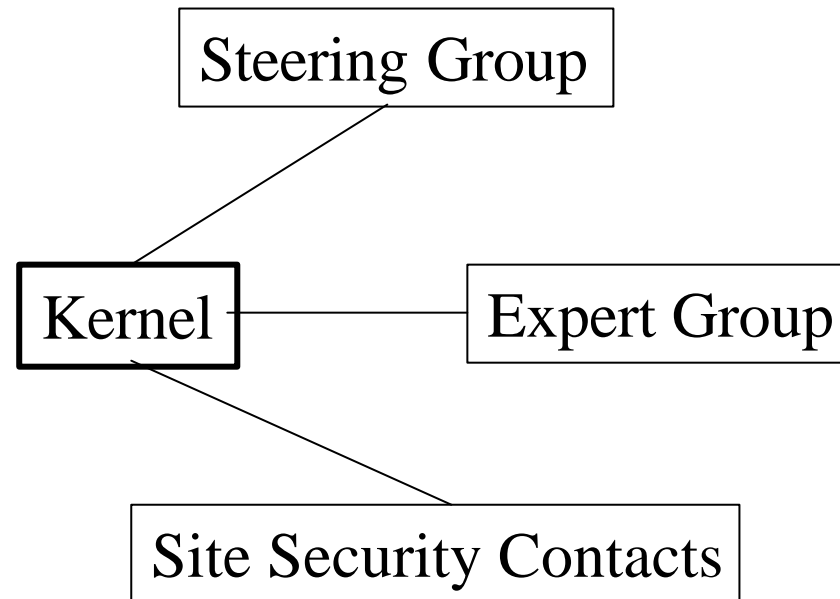
CERT -NL is the Computer Emergency Response Team of SURFnet, the Internet provider of the Higher Education institutes and many research organizations in the Netherlands. CERT-NL handles all cases of computer security incidents in which a SURFnet customer is involved as a victim or a suspect.

Since 1992

Main goals

- Incident Response 24x7
 - coordination between involved parties
- Education and awareness
 - advisories
 - seminars etc..

Organizational structure



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

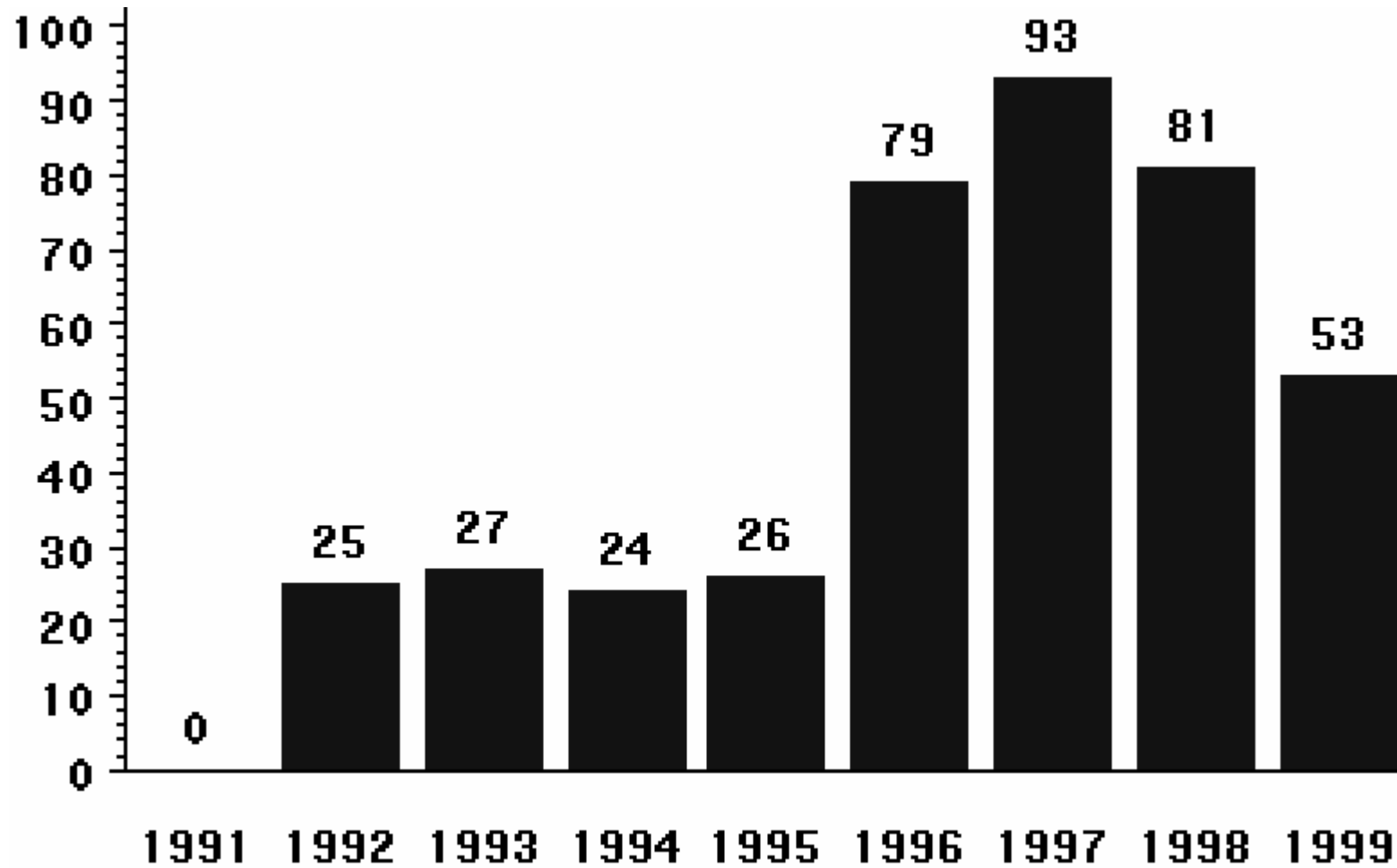
Case follow-up

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

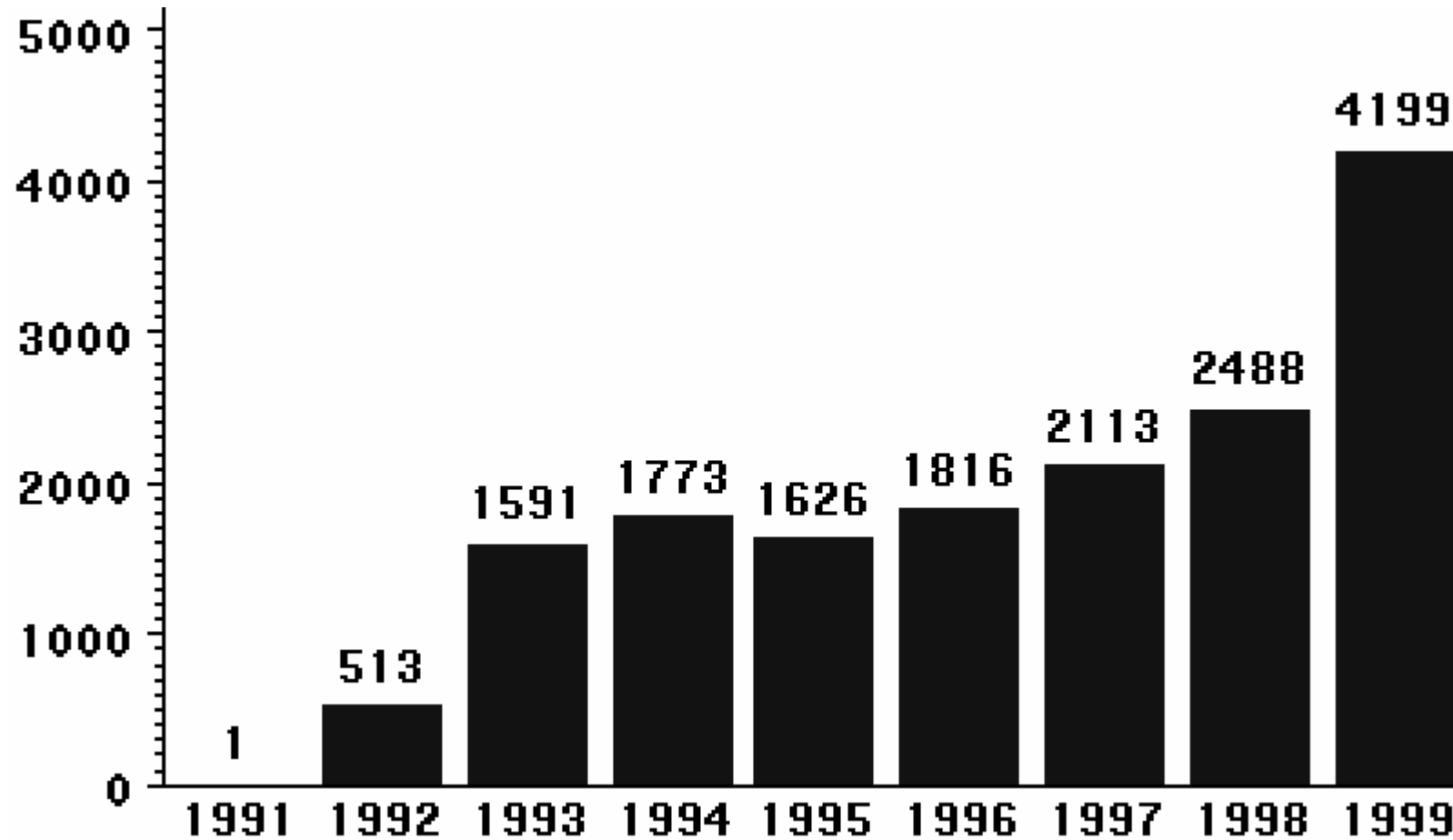
Tools

- 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



CERT-NL Mail



Logged events 1999

