SURFnet-CERT

A versatile Computer Security Incident Response Team

Jacques Schuurman

Chair SURFnet-CERT

Brussels, 13 December 2005

Agenda

Agenda
Introductie
Missie
Opzet
Werkwijze
Conclusie

- Introduction
- Mission and history
- Organisation
- Operation
- Conclusion

Remember?? (1/3)

Agenda
Introductie
Missie
Opzet
Werkwijze
Conclusie

- End 1988 - Morris worm:
  - "large scale"
  - automated
  - malicious
- Reaction from the Academic Community: foundation of Computer Emergency Response Team (CERT™)

Remember?? (2/3)

Agenda
Introductie
Missie
Opzet
Werkwijze
Conclusie

- 1991 – CERT-CC's example gets follow-up:
  - per country
  - per sector
  - per NREN (National Research and Educational Network)
- In NL: CERT-NL (founded by SURFnet; primarily for its own constituency, but nonetheless "best effort" for the rest of .NL

Remember?? (3/3)

Agenda
Introductie
Missie
Opzet
Werkwijze
Conclusie

- Initially: incident response
- Gardually buildig up experience:
  - operationally strong
  - tactically uncertain
  - strategically “unaware”
- Preaching fior our own parish
- Still: too few co-operation ties
  - (best case ad-hoc)

Gradually, the mission changes ….

Agenda
Introductie
Missie
Opzet
Werkwijze
Conclusie

- Adhere to common mission SURFnet:
  - not only *fire brigade*, but additionally:
  - *police* to "nasty" institutions
  - *ambulance* to "victimised" institutions
- More attention to strategic aspects
- Shift reactve -> proactve
- Common interest of our *constituency* better defended

…. working proactively is vital

Agenda
Introductie
Missie
Opzet
Werkwijze
Conclusie

- Establishing a point of contact who is deciding within their organisation
- A clear(er) definition on what is (not) allowed using the connection
- Setting an example in (inter)national context

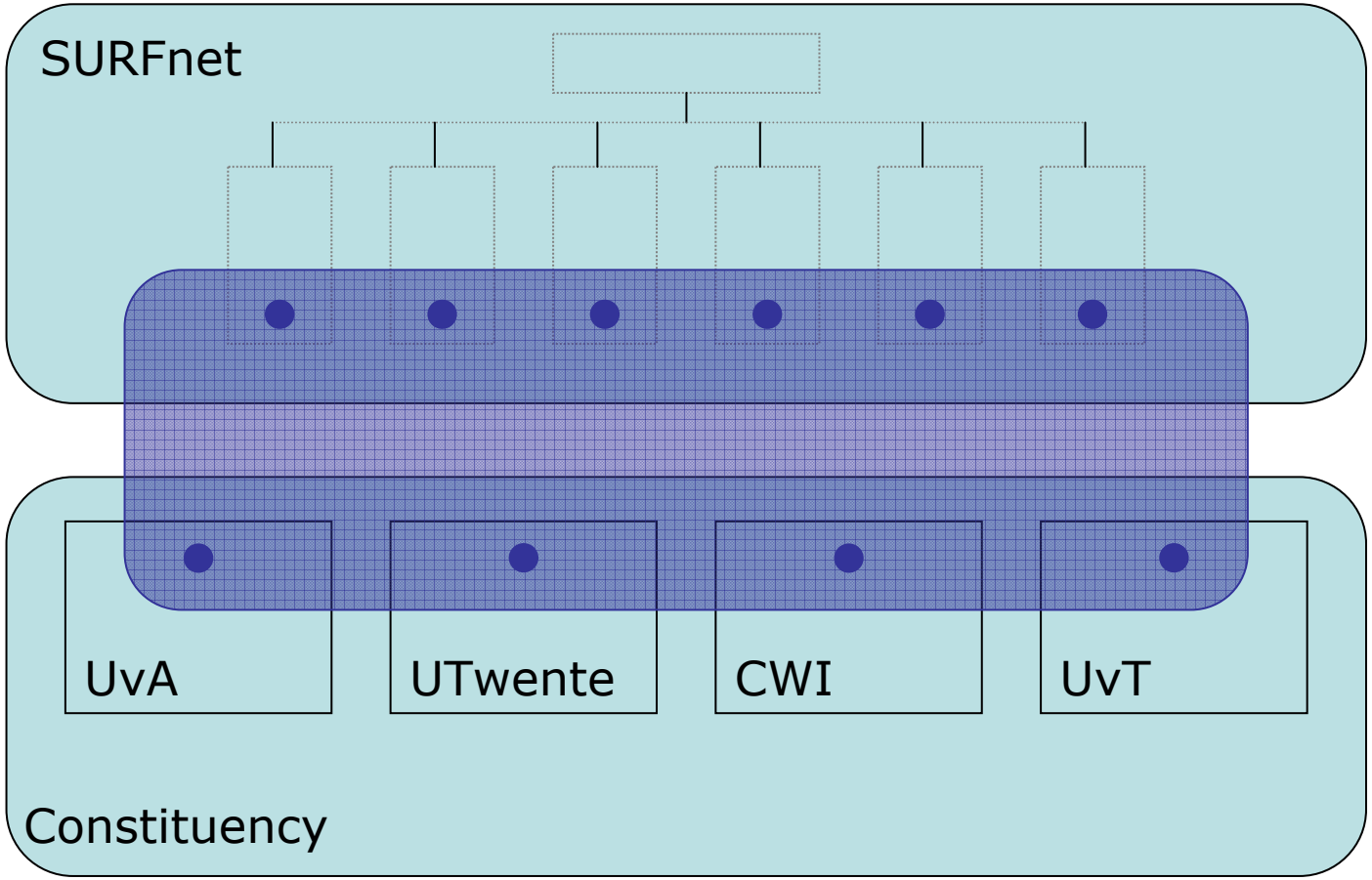
Organisation of SURFnet-CERT (1/3)

Agenda
Introductie
Missie
Opzet
Werkwijze
Conclusie

- Minimalising cost
  - no “idle time”
  - limited personal overhead
- Maximalising effectiveness
  - wide expertise
  - full availability (24x7)

Organisation of SURFnet-CERT (2/3)

Agenda
Introductie
Missie
Opzet
Werkwijze
Conclusie



Organisation of SURFnet-CERT (3/3)

Agenda
Introductie
Missie
Opzet
Werkwijze
Conclusie

- SURFnet:
  - Wim Biemolt (MWS)
  - Xander Jansen (CS)
  - Jan Meijer (MWS)
  - Luuk Oostenbrink (NWD)
  - Niels den Otter (NWD)
  - Jacques Schuurman (AA)
- Constituency:
  - Jaap van Ginkel (UvA)
  - Teun Nijssen (UvT)
  - Peter Peters (UTwente)
  - Jan-Philip Velders (CWI)

Operational practice (1/2)

Agenda
Introductie
Missie
Opzet
Werkwijze
Conclusie

- Available 24x7:
  - On duty (pager)
  - reachible via dedicated phone number
  - obviously via **cert@surfnet.nl**
- All complaints be administered through, well-defined ticket-systeem
- Workload on duty: app.. 24-32 uur
- Workload after hours: p.m. (1-2 uur)

Operational practice (2/2)

Agenda
Introductie
Missie
Opzet
Werkwijze
Conclusie

- Received complaint:
  - relevance (SURFnet-address involved)
  - triage (what type of incident?)
  - urgence (damage, impact)
  - coördination/assistence
  - Closing
  - statistical analysis

Some tactical considerations

Agenda
Introductie
Missie
Opzet
Werkwijze
Conclusie

- Cooperation fames:
  - formalised
  - informal (“small community”)
- Trust relationships:
  - by means of accreditation
  - equipped to tools
- Generally:
  - exchange on basis of “need-to-know”

Strategic ambitions (1/3)

Agenda
Introductie
Missie
Opzet
Werkwijze
Conclusie

- More services:
  - PACT (accreditation and tooling)
  - NERD (analysis of NetFlow data)
  - IDS ("weather chart" and noise measurement)
  - AIRT (unified administration and taxonomy)
  - "Kennismiddagen" (quarterly seminars)

De strategische ambities (2/3)

Agenda
Introductie
Missie
Opzet
Werkwijze
Conclusie

- Working with the constituency:
  - BCP's, dissemination, …
  - facilitating of "early adopters"
  - exposure and PR
  - second opinion for "large" incidents

De strategische ambities (3/3)

- Peer-to-peer cooperation:
  - national (IBO, o-IRT-o, OM, NHTCC)
  - international (TF-CSIRT, FIRST, GÉANT)
  - incidental (accreditation, …)

Concluding....

Agenda
Introductie
Missie
Opzet
Werkwijze
Conclusie

- Internet is defined to be a critical infrastructure;
- Management of this is done privately(!);
- Self-regulation is necessary and unavoidable;
- SURFnet-CERT is an implementation of this principle
  - reactive (keeping the net clean)
  - proactive (support the constituency)
  - policy making (advising)

ENISA: an important partner!

position, scale, view