

Full Security Capability: a Collective Effort

Jacques Schuurman

TF-CSIRT, Istanbul, TR, 17 September 2010



Est. 2011
Editor in Chief: Mary Smith

Internet Daily

Internet weather:
Xatlantic congest.

Thursday, 12 July 2012

43,000 student records including sensitive financial and medical information on loose

Data Disaster at DD University

Amsterdam, 12 July 2012 – **Malicious hackers have succeeded in breaking into the student enrollment system at DD Univ., an official spokesman confirmed. This system, certified to be “hack proof”, was procured by DD in 2011 for an investment of €4.5m.**

The major hack comes at a moment amidst student unions still raising concerns against new strict school regulations that require submission of financial and medical information in the enrollment process.



• *Head of ICT operations, Dr. Alan Feelgood, minutes before a press conference in which he announces his immediate resignation*



Outline



- Context of SURFnet
- Our view on Security
- Traditional paradigm
- Networked paradigm
- Concluding remarks

About SURFnet (1/2)

Empowering Innovation

- SURFnet enables and promotes groundbreaking education and research
- Designed and operates the hybrid SURFnet6 network
- Corporate Mission:
Providing advanced network technology for the .NL community of higher education and research



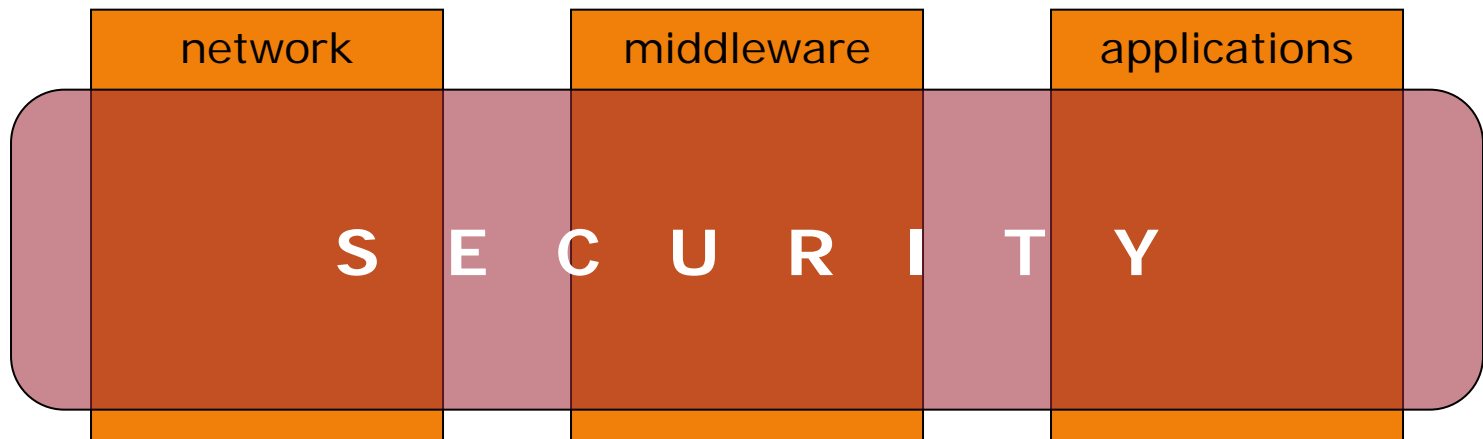
About SURFnet (2/2)

The SURF organisation

- SURFnet is a subsidiary of the SURF organisation, in which Dutch universities, schools for applied sciences, and research institutes collaborate nationally and internationally on innovative ICT facilities
- Ergo: we are **owned** by the **users** that we work for


Security for SURFnet

- Services are provided in three 'focus areas':
 - Hybrid network connectivity
 - Trusted Identity Management
 - On-line collaborative applications
- None of these per se secure in itself: security across all areas





Traditional paradigm

- SURFnet/SURFcert is 'provider' of security services
- Exclusively for the constituency
- Services include:
 - (traditional) incident response
 - (web based) tooling
 - providing advice on demand
 - training and awareness
- All of these above in a **one-way** fashion
- Very good results over the past 15-20 years
- One vehicle:  to become multi-functional



Networked paradigm: why?



- Certain security services become off-the-shelf available from the market:
 - anti-spam
 - workflow tracking systems
 - IDS-like systems
 - Flow (e.g. *NetFlow*) analysis software
 -
- Expertise available locally at institutes and SURFnet is not always deployed **efficiently**
- Security in itself is *meta* and auxiliary to the focus areas, but it requires **trust**, and SURFnet is in a position to facilitate that



Networked paradigm: what?



- Taking the existing **expertise** as a base line
- Engaging constituents into an active **community**
- Determining the sub-areas of security where **additional value** can be provided
- **Joining forces** towards external parties
- **Exchanging information** within the community:
 - best practices
 - war stories
 - operational information
- Certification **standards** (audits) for ICT infra:
 - data protection
 - incident management
 - identity management





Networked paradigm: how (1/2)?



- Setting up and facilitating a **community**:
 - SURFnet Coordinating Incident Response Teams (SCIRT) [yet another confusing acronym]
 - Founded in November, 2009
 - Community governing itself (independence)
 - Chair chosen internally **Ewald Beekman, AMC**
 - Non-disclosure agreement on an individual basis
 - ± 80 members representing ~40 institutes
 - Assembles every ~four months
 - Expert subgroups



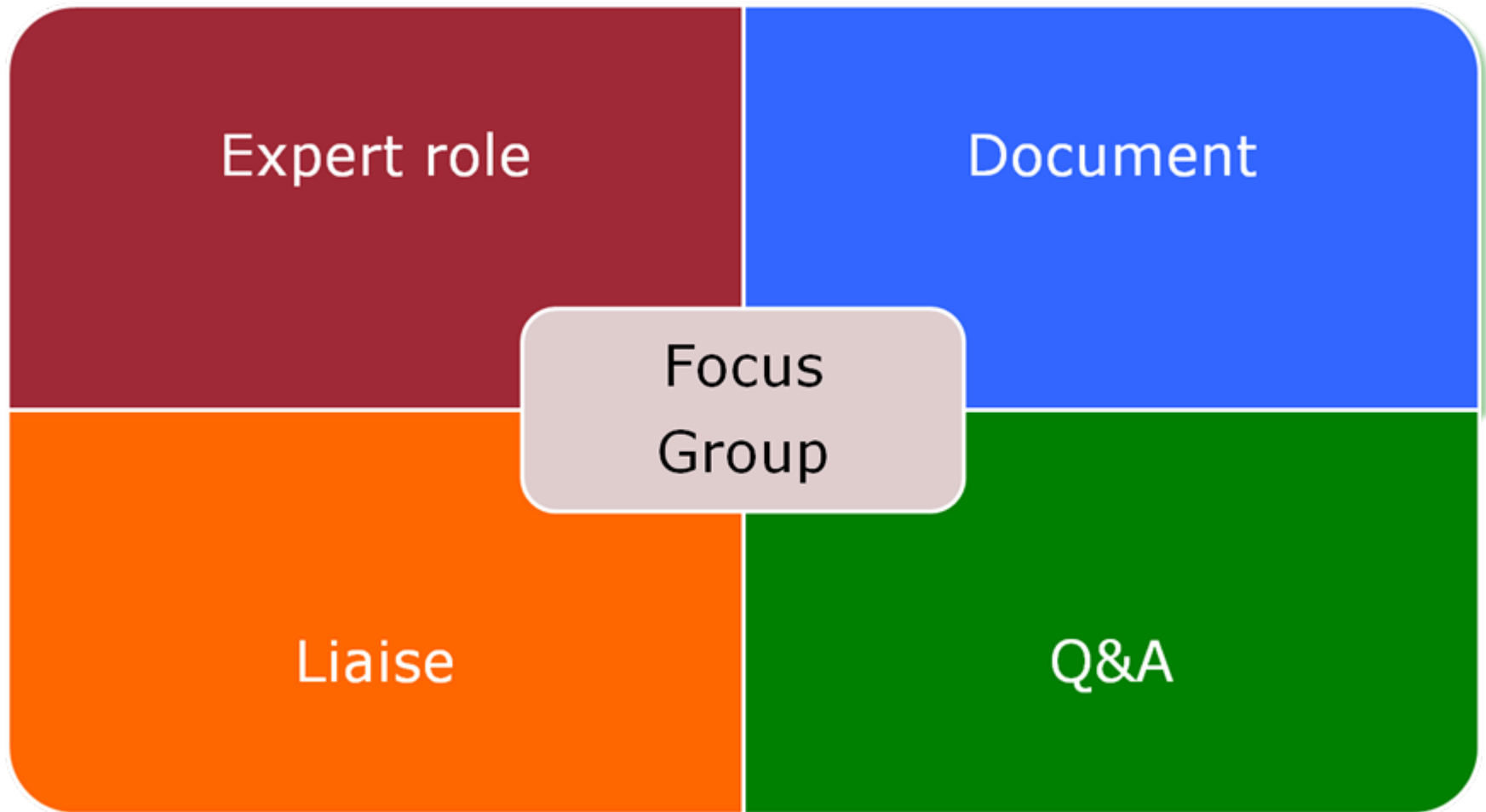
Networked paradigm: how (2/2)?



- **Expertise portal** on Security
- Aim:
 - reach-out to the broad constituency
 - continuously reviewed and maintained by SCIRT
 - in the end: SURFnet responsible
 - transparent dissemination of information and expertise in the field of security:
 - best practices
 - community news
 - white papers, cookbooks
 - acquiring input from various sources, also from outside the community



Focus Groups: Main goals



Existing Focus Groups



Software Audits

- coordinator: Jeffeny Hoogervorst (UvT)
- participants: 5



Juridische Vragen

- coordinator: Jacques Schuurman (SURFnet)
- participants: ?



Wifi

- coordinator: Raymond Mul (UvT)
- participants: ?

Coordinated Focus Groups



IPv6 Security

- coordinator: JP Velders (UvA)
- participants: 2



Honeytrap & IDS/IPS

- coordinator: Sebastiaan Tesink (UvT)
- participants: $3 + 5 = 6$



Incident en Risk Management

- coordinator: Ewald Beekman (AMC)
- participants: 4

Focus Groups Yet without coordinators



VMWare /Xen / HyperV / KVM / ...

- coordinator: ?
- participants: 5



Malware Analyse

- coordinator:
- participants: 4



Forensics

- coordinator:
- participants: 5



Phishing

- coordinator:
- participants: 3

Concluding observations

- Providing security **with** the community seems to be a feasible way forward
- Results –so far- look promising: SCIRT is actively engaged in working on expert deliverables
- In essence: paradigm shift from a 'vendor' position towards a 'partner' position
- No rocket science in itself, it however requires a different mindset with both NREN and institutes
- This approach might be easily applicable to other domains where expertise is an essential asset



Summary

- Traditional 'vendor'-'consumer' paradigm has worked for a long time; now eroding
- Various reasons for a shift towards a partnership paradigm (networked paradigm)
- SURFnet in a position as trusted facilitator
- Building and maintaining a community essential for success in the longer run
- First results encouraging: we seem to have chosen the right direction
- [jacques . schuurman @ surfnet . nl](mailto:jacques.schuurman@surfnet.nl)
- **Questions/Discussion**