Working with Authorities

Finding the balance in the force field of MUSTs, SHOULDs, CANs, SHOULD-NEVERs, CANNOTs

Jacques Schuurman
SURFnet-CERT

Amsterdam, 24 February 2006
Agenda

- The context
- Some recent “highlights”
- Near future
- Far future
- Conclusion
The context

The SURFnet perspective

- SURFnet: NREN with a closed user group
- Clients are institutes, so:
  - Legal entities of their own
  - *They* have end users, *we* do not
- SURFnet(-CERT):
  - Defines who are entitled to SURFnet services
  - Sets basic guidelines to what traffic is routed and what traffic is dropped
- Enforces aforementioned rules, both technically as well as legally
The context

The institute’s perspective

• SURFnet: A provider (as good/bad as any other??)
• We are institutes, so:
  – We determine for ourselves what is “good” and what is “bad”
  – We have end users, they do not (what do they care about end users anyway!)
• SURFnet(-CERT):
  – Is a pain in the ass and not flexible at all
  – Comes up with new rules and regulations every bl**dy week
• Blocks ports “at will”
The context
The end user’s perspective

- SURFnet: Whos is that? I get Internet access from my school!
- We are academic end users, so:
  - We know for ourselves what is “good” and what is “bad”, no interference
  - We are end users, they do not (what do they care about end users anyway!)
- SURFnet(-CERT):
  - Is a lousy provider (all sorts of nice and handy protocols simply do not work over their network)
- Blocks ports “at will”
The context

The authority’s perspective

- SURFnet: A provider with all the liabilities that go with it
- We are law enforcement, so:
  - We determine what needs to be scrutinised, and how, and when, and why
  - Of course, we do not communicate on this...
- SURFnet(-CERT):
  - Needs to assist us in any possible way, at any given time, 24x7, without undue delay
  - Is, in the legal sense, no more than an ordinary citizen, with no additional competence or capacity
Recent “highlights”
The matter of tapping capacity

- Telecom regulations: all “public” providers must maintain tapping facilities for the Law Enforcement authorities (exclusive access)
- The OPTA (Telecom Regulator’s Office) is the authority that determines whether a provider is “public”
- SURFnet -> OPTA: “We are not a public network” (mid 2003)
- OPTA -> SURFnet: .... (so far)
Recent “highlights”
Cooperation in a criminal investigation

- SURFnet connected institute hacked (big time)
- SURFnet-CERT to assist in initial investigation of the case
- Connected institute to file a case with the police (entrance into Law Enforcement circuit)
- Law Enforcement bodies are seeking the assistance of SURFnet-CERT in further instigation and forensics
- Complicated (and delicate) relationships between LE bodies and to the “outside world” unrevealed to us
- What MUST we do, what SHOULD we do, what CAN we NOT do? Potential liability works towards all the parties involved
Near future

- More confusion:
  - Unclear legislation
  - Untested legislation
  - Inconsistent legislation
- Finding the adequate positions and roles
  - Providers vs. end users
  - Copyright enforcers vs. providers
  - LE bodies vs. providers
  - LE bodies amongst themselves
Far future

- Internet (whichever generation) to become normal public infrastructure
- Better fitting and genuine legislation and rules adequate for this type of environment (including all types of transactions)
- More experience with the real application of applicable laws
Conclusions

- The cyberworld has some specific different characteristics (relative to the real world), relevant to the perception of how law enforcement should look like.
- Now, relevant bodies working with the law and law enforcement are (slightly) confused and look for a modus vivendi.
- Therefore, on short term we should continue to expect operational clashes, silly laws, and organisational misunderstandings.
- On a longer-term perspective, this will gradually converge to a sustainable environment where a balance is found.
Good news: social event sponsored!