To mean well is not the same as to do well

What’s wrong with the draft on NIS from a practical point of view

Florian Walther
Chaos Computer Club / CCC

What we face...

- Attacking central nervesystems of the net
  - Attacking DNS, routing protocols (e.g.BGP) and/or routers, Worms like *Conficker* for example
  - Big scale exploitation of systems as in take over the monocultures (Android)
  - Massive (d)DoS / flood the net

Conficker like threats

- You need ad-hoc interdisciplinary working groups. That is what has been proofed to be effective in earlier cases, like the conficker case.
- A self-established working group of malware researchers, network experts, agents,.... have worked together to deal with the threat.
- Make sure you have this flexibility when you need it.

What does the draft propose?

- Very breifly you could say, it proposes...
- Every Memberstate should have adequatly equiped and trained personel to deal with network security incidents.
- Memberstates should work together and share their information to hanlde incidents.
- The private sector needs to get involved because most systems are private systems

That was the good stuff

- Cooperation, training, skilled personel, redundant infrastructures for CERTs, information sharing, that’s all a good thing to do.
- Make sure all memberstates have adequatly equiped budget at hand for building a good CERT
- Work together with reasearchers and experts from academia, and the it-security scene.

...the draft also proposes...

- A confidential network of memberstates, involved agencies, organisations and companies
- Passing on personal data to other organisations and countries
- Keeping vulnerability information strictly confidential prioir to the availability of a fix is dangerous!

secrecy vs. transperancy

- Information about threats and vulnerabilities should be public information
  - If you do not know, you can’t react.
- In most cases secrecy does only harm cooperation and information sharing.
- Having confidentiality barriers will limit the effectivness, reach-out and support

No knowledge, no defence

„(28) [...]In the implementation of the notification obligations, competent authorities should pay particular attention to the need to maintain information about product vulnerabilities strictly confidential prior to the release of appropriate security fixes.[...]“

- What if a vendor does not fix the problem?
- What if there is no short term fix?
- What if there is no vendor?

No knowledge, no defence

- It’s OK to give vendors the chance to fix the problems they caused with their bad implementation / design descision / default settings /...
- In cases vendors do not cooperate you need to make it public without a fix, in certain emergency situations it could be better to release the full vulnerability information even there is no fix.
- The Internet is like an organism, once it knows about a threat it can strengthen it’s immune system

Vendors need public awareness to behave responsible

- Don’t wait for the fix by all means
- Give Vendors some maximum period of time (1 to 4 weeks) to deliver fix
- Go public with the vulnerability details that are important and needed to protect systems / identify attacks
- Not informing the public weakens network security and protects uncooperative and unresponsible vendors!

Security Contacts are helpfull

- Why there is no obligation on market operators to provide a public security contact, as proposed in RFC2142 Section 4 ?
- One of the problems in practice is to first inform institutions about their security problems
- Could be done in Article 14

Public interest at stake

- Article 14.4 :“The competent authority *may* inform the public, or require the public administrations and market operators to do so, where it determines that disclosure of the incident is in the public interest“
- Public interest is not a *may*, it is a *mus*t!

Data protection

- Article 13

„Such agreement shall take into account the need to ensure adequate protection of the personal data circulating on the cooperation network.“

Such an agreement must ensure best possible protection of personal data!

Article 15 (2/3) no safegaurds

- (2) Public administrations and market operators can be forced to undergo a security audit and provide security information about their assets.
- What for? I miss appropriation for this point!
- (3) issue instructions on market operators
- That should be more precise in order to only allow instructions to strenghten it-security.
- These instructions must be questionable in court.

Obligated security audits

- Who has to pay?
- How often this can happen?
- Smaller market operators should be protected from pushed to bancrupcy due to this obligation.
- Also it need to be defined much more precise what can be obligated under what circumstances and how often.
- Also who gets access and for what reason to audit results needs to be defined proper.

What i missed in the draft
- Water supply -

- Anyone thought about one of the most critical infrstructures for human beeings – water suply?
- Why is water supply not mentioned in this draft?
- Do you think water is nowadays supplied without using computers?
- Wake up!

Hard- and Software vendors

„Software developers and hardware manufacturers are not providers of information society services and are therefore excluded.“

Well but they have to fix the vulnerabilities that are the root cause for most NIS incidents.

So you need them hold responsible to fix what they have done wrong in their products.

Without the vendor help you will not go anywhere with network security in europe.

Thank you

Florian Walther

fw@snurn.de