

A large red devil icon with horns and a tail, serving as a background for the text. The tail is a thick red line that loops around the text and ends in an arrowhead pointing downwards.

BOFH

DNS whitelists for e-mail

September 25th 2009 – TF-CSIRT – Tallin, Estonia
JP Velders – UvA & SURFcert



DNS based lists

- Mostly used: DNS **black** or **block** lists
- Can be used to convey a lot of information
- Easily queried from various systems
- Most mailsystems already support DNS based list lookups, both for stopping or allowing mail to be delivered



E-mail and DNSwl's

- Especially the academic world has a need for widespread e-mail contacts (no use in blocking China or \$BadCountryOfTheDay)
- Some NREN's are running large mailfilter setups (SURFnet does, not all customers use it though ☹)
- Whitelisting infrastructure could benefit the academic community greatly



Academic only ?

- Need to start somewhere to see if it works
- DNSwl.org could incorporate the list
- To be of use some ground rules are necessary, under a CSIRT's supervision
- Rol evident



Policy (1)

- V0.3, written in 2006 (!)
- Gives some assurances
- No “free meal”
- NREN/CSIRT
 - Update details
 - Respond adequately
 - Take measures when needed



Policy (2)

- Constituent:
 - Be pro-active
 - Take complaints seriously
 - Keep information up-to-date
 - Good Netizen-ship
 - Configure mailservers to some sane defaults



Work so far

- Limited proof of concept
- <http://eunrendnswl.uva.netherlight.nl/>
- Small Postfix daemon to query
- Uses a CSIRT + constituent model
- Dumb MySQL database
- Needs input from actual use



Discussion

- Who would like to actually participate ?
- Critical mass needed !
- Eduwhitelist.org up for renewal soon...
- Build up infrastructure (involve TERENA for NREN's ?)



JP Velders <J.P.Velders@UvA.NL>
UvA & SURFcert