

Setting up a DNS-CERT our opinion

Shantha Fernando
CEO, TechCERT
a division of LK-Domain Registry



Contents

- Background
- Can DNS vulnerabilities be isolated?
- Why CERTs?
- How do they operate?
- Where would a victim call?
- Implications
- Our recommendations
- Conclusion

Background

- Proposal to set up DNS-CERT
 - Initiated by ICANN
 - Lot of funds to be allocated
- Discussion on DNS-CERT
 - Many stakeholders expressed the views
 - The need to address escalating DNS issues were accepted
 - However, many opposed the way it was proposed to be done

Can DNS vulnerabilities be isolated?

- Nature of computer and network security issues
 - Most of the time they do not happen in isolation
 - interconnected with vulnerabilities in networks, applications and organizational procedures

Why CERTs?

- To cater for all types of computer and network security incidents
 - Very first CERT was set up as a response to an attack due to vulnerabilities in BIND, however, interconnected with many issues related to system administration
 - Not only DNS admins

How do they operate?

- Coordinate with other CERTs
 - Sometimes, regional efforts
 - e.g. APCERT
- Autonomous operations
 - CERTs in different countries follow different models
 - Yet they share information and collaborate in security issues and incidents

Where would a victim call?

- How would one find the proper CERT to call?
 - In an emergency, any CERT can be called
 - Any CERT should provide immediate response
- Would the victim know whether the problem was with DNS or something else?
 - In some cases, would even a CERT know before a research is done?



Hence the implications are

- Boundaries of DNS-CERT scope seem to be ambiguous
 - Ultimately it will end-up being a general CERT
- It does not seem to be logical for ICANN to specify what CERTs should do
 - Rather it is autonomously, yet collaboratively handled by each CERT

Our recommendations

- If any regional effort is needed, may be collaborative affiliations can drive it forward
 - e.g. APCERT
 - May be, for the next APTLD meeting, APCERT can be invited
 - Further, get the existing CERTs involved with APTLD in a formal manner

Conclusion

- Let the existing close collaboration between CERTs be not disturbed but strengthened !

Thank you

Shantha Fernando

