Update on ICANN Security, Stability and Resiliency Programs and Activities

Greg Rattray
ICANN Chief Internet Security Advisor
10 March 2010

Strategic Initiatives - Background

- Growing risks to DNS security and resiliency
  - Emergence of Conficker; growing domain hijacking
- Community calls for systemic DNS security planning and response
- ICANN commitments under Affirmation of Commitments
- Initiatives called for in ICANN 2010-2013 Strategic Plan

Organizational/resource approaches not predetermined

Initiative #1 – System-wide DNS Risk Analysis; Contingency Planning; Exercises

- Envisaged as a Community-based effort; supported by ICANN
- Risk framework and regular risk assessment
- Root sever information sharing system
  - Based on concerns raised in root scaling study
- Contingency planning based on key scenarios
- Initiate a system-wide DNS exercise program
  - Build on existing efforts

Initiative #2 – DNS CERT (Computer Emergency Response Team)

- Validated need for standing collaborative response capability to address systemic threats/risks
  - Full-time/global; coordinate existing capabilities; serve all stakeholders especially less resourced operators
- Operational focus determined in engagement with stakeholders and leveraging existing efforts
  - Fostering situational awareness; incident response assistance /coordination; support efforts under Initiative #1

More fully developed DNS CERT Business Case posted along with Strategic Initiatives paper

Way Forward on Security Initiatives

- Seek community feedback
  - Consultation occurred Monday at Nairobi meeting and discussed with GAC
- Address organizational and funding approaches

DNS System-wide SSR Coordination, Analysis and Planning

- Revising *ICANN Plan for Enhancing Internet Security, Stability and Resiliency*; basis for upcoming Affirmation of Commitments review
- Conducted 2nd annual DNS SSR symposium in Kyoto in early February focused on Measuring DNS Health.
  - Over 50 expert participants focused on describing key DNS health parameters
  - Baselining what metrics and measurements exist and where gaps exist in terms of getting more comprehensive. Symposium report forthcoming
- Developing set of key contingencies for use in ICANN and community efforts related to response and exercise planning
- Finalizing gTLD continuity plan to address how to protect registrants

Mitigation of Malicious Conduct in New gTLDs

- Measures included in current draft applicant guidebook include requirement for DNSSec; prohibition on wildcarding; requirements for background checks on applicants.
- Work group on establishing a scalable approach to Zone File Access
- Working group on establishing a voluntary High Security TLD verification program.

DNS Collaborative Response

- Working closely with FIRST and national CERT community
  - Joint session; 35 students; help set up East African CERT
  - Plan survey on ccTLD – national CERT collaboration
  - DNS Security workshop at FIRST general meeting in June
- Continue collaboration in stopping spread of Conficker as well as lessons learned and follow-up efforts
- Continue to have security team incident reporting mechanisms to identify potential systemic DNS incidents

TLD Training Programs

- Continue conduct of ccTLD security and resiliency training program
  - Attack and Contingency Response Program focused on managerial level threat awareness and contingency planning conducted in Seoul, Korea and Amman, Jordan
  - Joint ICANN/ISOC registry operations training program initiated focused on basic, advanced and security DNS technical skill building . Sessions have included Santiago Chile; Dakar, Senegal; and Nairobi Kenya – 25 people; 8 ccTLDs
  - Reaching over 100 DNS ccTLD operators in 41 ccTLDs in the last six month in conjunction with regional TLD associations

Global Engagement

- Work closely with regional TLD associations to include consulting on DNS-CERT concept
- Work closely with Global Partnerships team to enhance regional outreach activities.
  - INTERPOL workshop
  - Asia-Pacific Economic Cooperation – Telecommunications and Information Working Group
- Major annual ICANN – Russian Institute for Information Security Issues forum in April