ICANN SSR – DNS Risks
Internetdagarna 2010

26 October 2010

Patrick Jones

Security, Stability, Resiliency (SSR)

- Key Operational priority for ICANN & a Core Value – Preserving & Enhancing the operational stability, reliability, security & global interoperability of the Internet

- FY 10-13 Strategic Plan, SSR one of 4 Strategic Focus areas
- ICANN's SSR programs and activities to be closely reviewed as part of the Affirmation Review on Security & Stability (Oct 2010)

ICANN Strategic Plan 2010 to 2013 - Four Strategic Focus Areas

Supporting... One World. One Internet. Everyone Connected.

	DNS stability and security	Consumer choice, competition and innovation	IANA and core operations	A healthy Internet eco-system
Strategic objectives	▪100% DNS uptime ▪Lower DNS abuse ▪More secure top level domain (TLD) operations ▪Improved DNS resilience to attacks	▪Everyone connected ▪Increased TLD options in more languages ▪Lower registration abuse ▪Increased industry competition ▪Increase valid registrations	▪Flawless Internet Assigned Numbers Authority (IANA) operations ▪Improved resilience ▪Enter into a long term IANA functions contract	▪One unified, global Internet ▪All stakeholders have a voice ▪Improved accountability and transparency ▪Enhanced trust in ICANN's stewardship
Community work	▪Domain name system security extensions (DNSSEC) ▪Whois/ International Registration Data ▪Addressing Registration abuse	▪IDNs ▪New gTLDs ▪IPv4/ IPv6 work ▪Registrar Accreditation ▪Registrant Rights Charter	▪Monitoring of performance ▪Root scaling study	▪Increasing participation ▪Contributing to international forums ▪Review SOs and ACs
Strategic projects	▪DNSSEC implementation ▪Establish DNS CERT ▪Contingency planning & exercises ▪IPv4 and IPv6 adoption	▪Implement Internationalized Domain Names (IDNs) ▪Implement new TLDs ▪IPv4 monitoring/IPv6 leadership ▪Improve policy processes	▪IANA infrastructure upgrade ▪Monitor Root scaling ▪Strengthen International operations and presences ▪ Strengthen SO and AC Support	▪Implement Community Reviews, including the Affirmation of Commitment reviews ▪Efforts to meet commitments ▪Implement impact reporting ▪Participate in Internet governance dialogues including Internet Governance Forum (IGF)
Staff work	▪Contingency planning ▪Training for ccTLDs ▪Collaborative response ▪ccTLD and risk management education in developing countries	▪Compliance ▪Supporting Organization (SO) and Advisory Committee (AC) support	▪IANA ▪Board support ▪Financial operations ▪Security & contingency ops ▪L Root operations	▪Thought leadership ▪International forum participation ▪Build capacity & strengthen partnerships across eco-system ▪Strengthen regional engagement

Multi-stakeholder – Collaborative – International – Transparent – Accountable

ICANN's Role

- Act in accordance with its bylaws in conducting multi-stakeholder, consensus-based processes, policies and programs.
- Focus on core mission related to the Internet's unique identifier systems
- Participate in activities with the broader Internet community to combat abuse of the unique identifier systems

Previous Activities & Issues

- ICANN Los Angeles – Nov 2001 focused on Security
- Created Security & Stability Advisory Committee (SSAC) - 2002
- Sitefinder – 2003; Wildcards & synthesizing of responses
- DDoS attacks (against registries, registrars, root operators, organizations & businesses)
- RegisterFly (registrar failure & termination)
- gTLD Registry Failover & Continuity exercises – 2006-present
- Global DNS SSR Symposium in Feb 2009 (Georgia Tech), Feb 2010 (Kyoto)

Threats & Risks to the System

- Large scale DDoS, leveraging the DNS for malicious activity
- Cyberattacks on Estonia (2007)
- Conficker/Zeus/botnets
- Social engineering attacks; Man in the Middle attacks
- URL shortener attacks
- Organizational risks from business failure
- Routing errors
- Stuxnet
- Natural disasters

Strategic Initiatives

- Feb 2010 –Strategic Initiatives paper; Global Business Case for DNS-CERT
    - Community-based approach to system-wide DNS risk assessment
- Apr 2010 – Operational Requirements & Collaboration Workshop
- May 2010 – Summary & Analysis of Comments posted
- June 2010 - ICANN Brussels meeting

Strategic Initiatives

- DNS-CERT was envisioned to provide proactive & reactive services to enable time & efficient response to threats to the security, stability & resiliency of the DNS
  - Proactive (threat analysis, monitoring, situation awareness, info sharing)
  - Reactive (incident handling coordination, support to resource constrained community, 24-hour point of contact)
  - Global scale
  - Improve communication within DNS operational community & broader security community

Going Beyond DNS-CERT

- The community has been clear –
  - "The requirements for a DNS-CERT must be analyzed in light of deeper understanding of the threats and risks to the DNS, and such analysis should precede specific proposals for a DNS-CERT."

Going Beyond DNS-CERT

- What's Next?
  - Staff supporting community-led discussion in Joint Security & Stability Analysis Working Group;
  - Birds-of-a-feather discussion on needs for collaborative capabilities for DNS incident handling;
  - Risk Assessment with experts

A Look Ahead

- Dec 2010 – ICANN Cartagena de Indias
    - Jan/Feb 2011 – ICANN DNS Ops/L-root Contingency Exercise
- March 2011 – ICANN San Francisco
- June 2011 – ICANN Asia-Pacific
- October 2011 – ICANN Africa

Upcoming Activities

- Community consultations at ICANN 39 in Cartagena on SSR; Joint Security & Stability Analysis Working Group
- Affirmation Review on SSR
- Participation in International cyber exercises
- High Security Zone Verification Program (HSTLD)
- Collaboration with root operators on root scaling, IPv6 introduction, IPv4 run out
- IDN variants and IDN table activities
- DNS Operations and L-root contingency exercise

More Information:
icann.org/en/security/