Strategic Initiatives for Security, Stability and Resiliency

Greg Rattray/Yurie Ito

Thursday 23 June 2010

Background

Growing risks to DNS security and resiliency

- Emergence of Conficker; growing domain hijacking

Community calls for systemic DNS security planning a response

Initiatives called for in ICANN 2010-2013 Strategic Pla

Organizational/resource approaches not predetermined

tiative #1 - System-wide DNS Risk Analysi
Contingency Planning; Exercises

- 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

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

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

Strategic Security Initiatives/DNS CERT: State of Play

DNS CERT Operational Requirements Worksho
April

Posting of Documents

- Summary of Comments; Workshop report; Lis
  Consults

Exchange of Letters with ccNSO/GSNO/ALAC

- Call for and preparation steps for working gro

Discussion of two-tier model for organization fo
supporting DNS-CERT

Risk Assessment, Contingency Planning & Exercise: Main Themes

Not a focus of comments

Generally supportive of need for risk assessme

- As step prior to launching CERT

Limited comment supports for concept of "cul
of preparedness" and contingency planning

Strategic Security Initiatives
CERT: Main Themes

- Topic worth discussing
- Need deeper understanding of threats & risks
- Understand current response capabilities
  - Does this overlap with current CSIRT capabiliti
  - Focus on strengthening CSIRT capabilities
- Limited response capabilities in less-resourced reg

Strategic Security Initiatives/DNS CERT - Proposed Next Steps

- Work on threat and risk understanding
- Continue to work with FIRST/CISRTs; initiate National CERT survey with CERT/CC
- Recognize desire ICANN not operate; focus o working with others and facilitating dialogue
- Discuss workshop and Conficker reports

Requirements & Collaboration Analysis Workshop

Group of operational security and DNS experts

- ICANN staff selected; qualifications provided

Conducted use case-based analysis

Report drafted by three participants, reviewed by all

- Included an alternative view

Provides basis for further community discussion

http://www.icann.org/en/public-comment/#dns-collab-analysis

Requirements

- **A trusted communications channel**
- **Standing incident coordination and response functions**
- **Incident status tracking**
- **A trust broker or introduction service**
- **Analysis capabilities**
- **Institutional memory**
- **A trusted voice for guidance on security matters**

based on Risk Areas for DNS

- Protocol/Code Vulnerabilities
- Registration Infrastructure Compromise
- DNSSec Key Compromise/Failure
- Registration Infrastructure Failure
- DDoS
- Malicious use of DNS

Existing Players

DNS OARC

OPS-Trust

nsp-sec

Conficker Working Group

FIRST

Regional CSIRT frameworks

NX.domain

Digital Crime Consortium

ISC SIE

- **SSAC and RSSAC mailing l**
- **ICANN**
- **NANOG and other region network operator groups**
- **MAAWG**
- **APWG**

Registration Infrastructure Security Group (RISG)

Produced by ICANN staff

- Vetted by Conficker working group

Way Forward – for ICANN staff efforts

- Formalize relationships between responders
- Put in place appropriate rapid response processes – ERSR
- Improve contact information with appropriate parties and incident response procedures

p://www.icann.org/en/security/conficker-summary-review-07may10-en

SSR Initiative: Way Forward

Support efforts related to systemic DNS risk assessment, contingency planning & exercises

- Is a structured, time-limited effort needed?

Support community dialogues on DNS-CERT requirements, possible organizational structures a resourcing models

- Including possible SO/AC working groups