Domain Name Registration and Operational Best Current Practices

Florian Maury
ANSSI

May 10, 2015

Document Motives

Motives :

- lack of documentation meeting our criteria
  - in French
  - independant
  - all-in-one
- incidents keep on occurring
- asked for by operators

A Broad Approach

"Risk management"-oriented approach :

- to identify vigilance points when contracting with a provider

A broad approach :

- DNS essentials reminder
- **organizational** aspects
- **legal** aspects
- **operational** aspects

Organizational Aspects

Registry Selection Criteria

Registry selection is **paramount** to secure a domain name

Registries are high-priority targets for attackers.

Expected security features (in addition to all availability best practices) :

- DNSSEC support
- **registry lock**

Our Vision of the Registry Lock

Registry lock :

- all domain-related information are **frozen**, including **delegations, DNSSEC material, whois content**

Procedure :

1. lock activated by the domain name holder
2. lock enforced by the registry
3. may be **unlocked only at the domain name holder request** :
   - the registry authenticates the request origin

Registrar Selection Criteria

Registrar selection is **as much important** as the registry selection

Expected security features :

- 2-factor authentication with access logs
- registry lock support
- DNSSEC support

Other Providers Contracts

Expectations of DNS hosting operators :

- application of technical best current practices

Expectations of resellers and other service providers :

- contracting is a **risk transfer**, not necessarily **risk handling** !

Legal Aspects

Legal Systems and Languages

Select registries and registrars subjects to legal systems and dispute resolution policies well-understood by the domain name holder.

Technical Aspects

Resiliency Axis : System Administration BCP

System administration BCP :

- implement a **backup** policy
- automate system **health-checking**
- set TTL values according to the operational needs

Resiliency Axis : State-of-the-art Compliance

State-of-the-art compliance :

- **TCP** support
- **EDNS0** support

Resiliency Axis : System Hardening

System hardening :

- deploy **DDoS mitigation** solutions
- **harden** operating system, not only the DNS service
- implement **role separation**
- implement **information compartmentalisation**

Resiliency Axis : Avoid SPOF

Avoid single points of failures :

- implement software **diversification**
- adopt a resilient **network topology**
- adopt a resilient **physical topology**

Limit third party dependancy :

- **avoid glueless delegations**

DNSSEC Recommendations ?

What about DNSSEC ?

- DNSSEC may be considered **once all of the above are applied**
- ANSSI resiliency observatory : **study DNSSEC** and its deployment

Q & A

Call for feedbacks :

guide.dns@ssi.gouv.fr

Google translated english version of the guidelines