The Middle East Space

Online Virtual Meeting on Thursday 10 March 2022

DNSSEC Signing and Validation

Statement

We, the Middle East Space community members, participating in the Internet Corporation for Assigned Names and Numbers Public meeting 73 (ICANN73) addressed the concerns of the DNSSEC (DNS Security Extension) signing adoption and enabling DNSSEC validation for the ME countries to contribute to safeguarding the global and united Internet and came up with this statement.

DNS is critical to ensure service continuity. Faulty or ineffective DNS services can negatively affect the perception of any organization (from clients, partners, or employees), impact your e-commerce applications, resulting in a loss in revenue, and ruin a brand image: 63% of organizations suffered app downtime as a direct result of a DNS attack last year.

Since the DNS is essential to the operation of the Internet, protecting the data provided by the DNS is critical as to help make good progress in DNSSEC signing and validations, we recommend that:

A. ICANN

a. Encourages ICANN community members (UASG, ALAC, GAC, etc.) to join and involve more with other groups working on DNS and DNSSEC outside ICANN for knowledge exchange and experience sharing.

b. Addresses and promotes the use of DNSSEC to secure the way information moves around the Internet.

c. Has an open discussion about the challenges faced and best practices with the countries and organizations that have implemented DNSSEC to achieve full implementation.

d. Conducts a study about the roles of different stakeholder groups such as Internet end-users, software providers, (IDN) ccTLD operators, technical and academic communities, governments, private sector, etc. to further promote DNSSEC.

e. Conducts sessions of identifying the ROI (Return Of Investment) in DNSSEC deployment and resolving and the ROR (Return Of Risk) About delaying the DNSSEC deployment and resolving.

f. Supports in developing protocols that will allow the DNSSEC process to be automated in the future.

g. Training local initiatives trainers on "DNSSEC validation and signing" to help other stakeholders to implement it, increase the security awareness level about dependence on DNS for the functioning of the Internet, and How costly is the exploitation that occurs if we don't have this protection.

h. Spreads the knowledge that DNSSEC not only protects "end-users, governments .. etc" but also could create opportunities for innovation and enable new technologies, services, and facilities.

B. TLDs (Registry, Registrar)

i. Start enabling the entry of DNSSEC data for registered domains in an automated and easy way.

j. Promote the concept of authenticity and integrity after enabling DNSSEC.

k. Identify which stakeholders need to secure their domain names and Conduct an awareness session, especially those who have the most popular online applications, brands, services,.... to increase the security awareness as a first step than going to other domain holders.

l. Plan training for registry and registrars administrators to manage the signing keys and a roll-over plan.

C. Network Operators

m. Enable DNSSEC validation on the resolvers that handle DNS lookups for subscribed users.

D. Internet Users (Registrants)

n. Start enabling DNSSEC for their domains.

o. Spread the knowledge to their organization about what DNSSEC is and why DNSSEC is critical for the security of the DNS.

We want to thank all those working hard to push the DNSSEC Signing and Validation project forward. We hope that these recommendations are considered to make significant progress.