Supreme Council of Information & Communication Technology
المجلس الأعلى للاتصالات و تكنولوجيا المعلومات

Internet Infrastructure Security Guidelines

The Supreme Council of Information & Communication Technology ‘ictQATAR’

2013

CS013

Table of Contents

Definitions and Abbreviations:

- **Botnets:** is a collection of compromised computers connected to the Internet, managed remotely.
- **BGP:** The protocol backing the core routing decisions on the Internet, specified in RFC-4271.
- **BCI**: Business Continuity Institute.
- **Critical Information Infrastructures:** A set of information technology and communications systems, services, and data assets, supporting Qatar's national Infrastructures.
- **CcTLD:** Country Code Top Level Domains, such as .QA
- **DNS:** The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to a network.
- **DRII**: Disaster Recovery International Institute.
- **DDoS attack:** An attempt to make a computer or network resource unavailable to its intended users or function.
- **Hosting Providers (Providers):** Commercial entities providing web hosting services for other businesses, entities or individuals.
- **ISO:** International Organization for Standardization.
- **ICANN:** A global non-profit organization responsible for coordinating the Internet's core systems of unique identifiers, most notably the Domain Name System (DNS).
- **Internet Service Provider (ISP**): A person that is licensed to provide one or more telecommunications services to the public or licensed to own, establish or operate a telecommunications network to provide telecommunications services to the public. This includes providers of information or content provided using a telecommunications network.
- **ictQATAR:** the Supreme Council for Information and Communications Technology
- **Malware:** Malicious computer content such as harmful scripts or pieces of code that could cause harm to the normal operation of the internet or internet dependent assets and/or users.
- **SBC:** Session Border Controllers are devices regularly deployed in Voice over Internet Protocol (VoIP) networks to exert control over the signalling deployed on the borders between two service provider networks in a peering environment.

1. Legal Mandate

Articles (4) and (5) of Decree Law No. (36) of 2004 establishing ictQATAR acknowledges the Supreme Council of Information and Communication Technology as the highest competent authority in the affairs of communications and information technology has the authority and competence necessary for the discharge of such affairs and in particular the authority to regulate and to make policies for the two sectors of Communication and Information Technology in the state of Qatar.

2. Introduction

The role of the Internet, in supporting the economy and in delivering information, education and entertainment are well understood and acknowledged. In light of the steady increase in sophisticated computer attacks on the internet infrastructures worldwide and in order to maintain the quality of this vital service, it is the responsibility of the government, and service providers to agree upon the baselines that ensure the Internet within the State of Qatar remain safe, secure and resilient.

The aim of this Internet Infrastructure Security Guidelines is to provide *recommendations* and promote baseline principles and controls to ensure that Internet infrastructure provisioning within Qatar meets the requirements of the community at large and service providers have clear guidelines on what is expected of them. Therefore this document aims to fulfill and stress upon the following objectives:

1. Increase confidence and usage of the Internet by the whole community, by ensuring high availability and resilience is *proactively* pursued.
2. Help Internet Service Providers (**ISP**s) and Hosting Providers (**Providers)** to deliver their services securely, with the highest levels of availability possible.
3. Ensure the internet services within Qatar provide a consistent level of availability and resiliency.

The basic principle that governs these guidelines is:

- To develop provisions that should lay the foundation and promote a resilient, safe and secure internet infrastructure and service.

3. Scope and Application

This document SHOULD apply to all:

- Internet Service Providers (**ISP**s) licensed to operate within the State of Qatar;
- Hosting Service Providers (**Providers**) operating within the State of Qatar;
- Sections of ictQATAR performing an operational Internet infrastructure related role such as ccTLDs.

Internet infrastructure security is a domain of paramount importance and magnitude, the guidelines and recommendations in this document only address areas that are most relevant and specific to our current needs.

4. ISP & Provider Infrastructure Security

4.1. **ISPs** and **Providers** SHOULD implement Business Continuity Planning Programs as per the [**IAP-GOV-INFA**] document section **9.2** or any similarly available international best practice such as **ISO** 22301, **DRI** or **BCI** practices.

4.2. **ISPs** and **Providers** SHOULD ensure that the internet infrastructure networks (design and components) and the associated technology specific services are adopting the vendor's best practices for disaster recovery and high availability.

4.3. **ISPs** and **Providers** SHOULD apply hardening best practices mentioned in [**IAP-GOV-INFA**] document section **2.5** "where appropriate" and the international and vendor specific hardening guidelines and best practices for the internet infrastructure backbone components such as: servers, authoritative **DNS**, internet gateways, core switches and backbone routers.

4.4. **ISPs** SHOULD not depend exclusively on a single vendor throughout the network infrastructure core.

4.5. **ISPs** SHOULD apply systems monitoring, change management and logging mechanisms best practices mentioned in **[IAP-GOV-INFA]** document section **10.2** for the internet infrastructure backbone components.

4.6. **ISPs** SHOULD apply detection and prevention technologies to ensure Internet feeds are free " as much as possible" from malicious traffic and activities like: **DDoS** attacks and **Botnets**;

4.7. IctQATAR is ready to cooperate with the **ISPs** to provide any technical guidance that may be required.

5. Internet Routing Security

5.1. **ISPs** SHOULD use authenticated external Border Gateway Protocol (**BGP**) sessions, **ISPs** SHOULD also consider employing authentication for internal **BGP** sessions.

5.2. **ISPs** SHOULD ensure that they carry out international and national peering to ensure resiliency of Internet feeds. **ISPs** should ensure they do not have single points of failure (Logical or Physical) from upstream providers, for example, by ensuring paths to upstream providers and Internet landing points are geographically and logically diverse.

6. Domain Name Services (DNS)

6.1. It's RECOMMENDED that **ictQATAR** and **ISPs** country-code TLD (**ccTLD**) servers and sponsored/unsponsored generic TLD (gTLD) servers:

a. Ensure there is no single point of failure in their service;

b. Restrict administration and management access to a secure local machine, no remote access should be allowed;

c. Change the administration password every 60 days and password complexity should be 12 alphanumeric characters at least;

d. Enable system access logging and change management logs for 6 month at least;

e. Use security-hardened servers whose security is proactively maintained and patched regularly as per the vendor's best practices;

f. Digitally sign their zones files;

g. Use cryptographic origin authentication and integrity assurance of **DNS** data;

h. Use cryptographic mutual authentication and data integrity of zone transfers and dynamic updates.

The recommendations above are an attempt towards ensuring the resiliency and security of DNS services in Qatar, and are aligned with the ICANN security agenda (**http://www.icann.org/en/groups/ssac/dns-security-update-1.htm)**; and the supporting technical readings (**http://www.icann.org/en/groups/ssac/reading**).

6.2. Cryptographic functions related to 6.2 (f), (g), or (h) above, SHOULD use a hardware security module for both key management and cryptographic processing.

6.3. **ISPs** providing recursive name services SHOULD:

a. Use security-hardened servers whose security is proactively maintained are used;

b. Ensure Services are provided to authorized users only (i.e., not open recursive).

7. Hosting Malware

7.1 **ISPs** and **Providers** SHOULD exert their efforts to ensure that **Malware** is not hosted, stored or made available in Qatar.

7.2 **ISPs** and **Providers** SHOULD ensure that their hosting guidelines (or similar) include the following provisions:

7.2.1 Content that contains malicious executable code is not allowed.

8 Handling Malicious Activity

8.1 **ISPs** SHOULD ensure that end-user devices, located within the State of Qatar, carrying out sustained attacks against the following are immediately quarantined from the Internet:

8.1.1 Qatar’s Internet Infrastructure, including:

8.1.1.1 Attacks on .QA name servers (ccTLD DNS servers), sponsored or unsponsored generic name servers (gTLDs DNS servers);

8.1.1.2 BGP related attacks;

8.1.1.3 Attacks on core infrastructure/backbone routers or service delivery infrastructure, including Voice over IP (VOIP) session border controllers (SBCs);

8.1.1.4 International Internet Gateways.

8.1.1.5 Qatar’s **Critical Information Infrastructures**.

8.2 **ISPs** SHOULD ensure that end-user devices, located within the State of Qatar, which are connected to the Internet and generating malicious traffic, are notified of the **Malware** problem. Devices that continue to generate **Malware**, seventy-two (72) hours after being notified SHALL be quarantined until the devices are cleaned by the service user. **ISP**s may refer the infected end users to http://call.qcert.org/ which is a call center established by ictQATAR to help end users clean their machines.

9 Take Down Notice

9.1 If ictQATAR has been made aware of a **Provider** hosting Malware contravening section 7 of this document, ictQATAR, after investigating the matter, MAY issue a written take-down notice to the **Provider**. On receiving the take-down notice the Provider and/or the ISP SHOULD remove the specific Malware or quarantine the relevant server(s) or take it offline, as soon as reasonably possible, but within a maximum of twenty four (24) hours from the time of receipt.