Broadband Infrastructure Security Policy

Ministry of Information & Communication Technology 'ictQATAR'

July 2014

Document Reference

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.
- **Broadband**: Internet access that offers more bandwidth than traditional dial-up access.
- **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.
- **MICT:** the Ministry of 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 Broadband dependent assets and/or users.
- **NIAP 2.0:** The National Information Assurance Policy version 2.0 issued by MICT
- **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(s)

Article 14 of Decree Law No. 16 of 2014 setting the mandate of Ministry of Information and Communications Technology (hereinafter referred to as "MICT") provides that MICT has the authority to supervise, regulate and develop the sectors of Information and Communications Technology (hereinafter "ICT") in the State of Qatar in a manner consistent with the requirements of national development goals, with the objectives to create an environment suitable for fair competition, support the development and stimulate investment in these sectors; to secure and raise efficiency of information and technological infrastructure; to implement and supervise e-government programs; and to promote community awareness of the importance of ICT to improve individual's life and community and build knowledge-based society and digital economy.

Article (14) of Emiri decision No. 27 of 2014 stipulates the role of the Ministry in protecting the security of the National Critical Information Infrastructure by proposing and issuing policies and standards and ensuring compliance.

The broadband infrastructure security policy has been prepared taking into consideration current applicable laws of the State of Qatar. In the event that a conflict arises between this document and the laws of Qatar, the latter, shall take precedence. Any such term shall, to that extent be omitted from this Policy Document, and the rest of the document shall stand without affecting the remaining provisions. Amendments in that case shall then be required to ensure compliance with the relevant applicable laws of the State of Qatar.

2. Introduction

The role of the broadband internet infrastructure, in supporting the economy and in delivering information, education and entertainment is 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 infrastructure within the State of Qatar remain safe, secure and resilient.

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

The aim of this broadband infrastructure security policy is to provide controls to ensure that broadband 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 broadband services 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.
3. Increase the level of security and privacy assurance in the internet infrastructure backbone.

The basic principle that governs this policy is:

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

Note: This policy document *replaces* the previously published guidelines (Internet Infrastructure Security Guidelines) issued in May 2013.

3. Scope and Application

This document SHALL apply to all:

- Internet Service Providers (**ISP**s) operating within the State of Qatar;
- Organizations rolling out internet broadband infrastructures "such as FTTH" and services "such as Hosting websites";
- Hosting Providers (**Providers**) operating within the State of Qatar;
- Sections of MICT performing an operational Internet infrastructure related role such as national DNS or ccTLDs.

4. ISP & Provider Infrastructure Security

4.1. **ISPs** and **Providers** SHALL implement Business Continuity Management Programs as per the [**NIAP 2.0**] document section **9** or any similarly available international best practice such as **ISO** 22301, **DRI** or **BCI** practices.

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

4.3. **ISPs** and **Providers** SHALL apply [product security] controls mentioned in [**NIAP 2.0**] document section **5** stipulating independent technology evaluation and security vetting for Broadband infrastructure backbone components *such as* Core switches, backbone routers, authoritative **DNS** and Internet gateways.

4.4. **ISPs** and **Providers** SHALL apply [Cryptographic Security] controls mentioned in [**NIAP 2.0**] document section **10** "where technically feasible" and the international and vendor specific security hardening guidelines and best practices for the Broadband infrastructure backbone components *such as* Core switches, backbone routers, and authoritative **DNS** and Internet gateways.

4.5. **ISPs** SHALL ensure the diversity of the core-networking infrastructure, using technologies from different vendors, eliminating Vendor Lock-in whenever possible.

4.6. **ISPs** and **Providers** SHALL apply systems monitoring, change management and logging mechanisms best practices mentioned in **[NIAP 2.0]** document sections **10 and 11** for the Broadband infrastructure backbone components.

4.7. ISPs and Providers SHALL ensure that support and maintenance conducted remotely from outside the state of Qatar is monitored and logged including of the support connection.

4.8. **ISPs** and **Providers** SHALL apply detection and prevention technologies to ensure Internet feeds for consumers are protected "as much as possible" from malicious traffic like basic **DDoS** attacks and known **Botnet activity**.

4.9. **ISPs** SHALL ensure that the provisioned networking home appliances installed for the users are configured/hardened according to the latest security best practices available at the time of provisioning and are not having backdoors, which may threaten user privacy.

4.10. MICT may facilitate technical guidance that may be required by sending your request online through http://www.qcert.org/contact-us

5. Broadband Routing Security

5.1. **ISPs** and providers SHALL use authenticated external Border Gateway Protocol (**BGP**) sessions whenever technically supported by partner peers. **ISPs** SHOULD also consider employing authentication for internal **BGP** sessions.

5.2. **ISPs** SHALL ensure that they carry out international and national peering to ensure resiliency of Internet feeds. **ISPs** SHALL 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. **MICT** and **ISPs** country-code TLD (**ccTLD**) servers and sponsored/unsponsored generic TLD (gTLD) server owners and operators SHALL:

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 SHALL be allowed;

c. Enforce robust password policies for all core equipment in accordance with the [**NIAP 2.0**] controls AM 19-22;

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 controls 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 6.1 (f), (g), or (h) above, SHALL use a hardware security module (HSM) for both key management and cryptographic processing as per the **NIAP 2.0** section **10**.

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

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** SHALL exert their efforts to ensure that **Malware** is not hosted, stored or made available in Qatar.

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

7.2.1 Content that contains known malicious executable code is not allowed;

7.2.2 Content that redirects users to known malicious servers is not allowed.

7.3 If MICT has been made aware of a **Provider** hosting Malware contravening section 7 of this document, MICT, 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** SHALL 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.

8 Handling Malicious Activity

8.1 **ISPs** SHALL 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;

8.1.2 Qatar's **Critical Information Infrastructure** organizations as defined in the Critical Infrastructure Information Protection draft Law.

8.2 **ISPs** SHALL ensure that end-user devices, located within the State of Qatar, which are connected to the Internet and generating malicious traffic, are notified by (Phone or Email) of the **Malware** problem. Devices that continue to generate **Malware**, seventy-two (72) hours after being notified SHALL be quarantined until the service user cleans the devices. **ISP**s may

refer the infected end users machines to http://call.qcert.org/ which is a call center established by MICT to help end users clean their machines.