وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

Cyber Security Guidelines for Securing Home and Small Office Routers

Version: 1.0

Author: CS Risk Management Section

Document Classification: Public

Published Date: March 2018

Document History:

Version	Description	Date
1.0	Published V1.0 document	March 2018

وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

Table of Contents

1 Legal Mandate(s)

Emiri decision No. (8) for the year 2016 sets the mandate for the Ministry of Transport and Communication (hereinafter referred to as "MOTC") provides that MOTC 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 (22) of Emiri Decision No. 8 of 2016 stipulated 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.

This guideline 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 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

Over the past decade, the Internet has shifted from a commodity to a necessity in every household in Qatar. Figures put the Internet penetration rate at 99% for households, and to achieve this connectivity, wired and wireless routers have moved into our homes.

These routers are provided by the Internet Service Provider (ISP), and are usually pre-configured and ready to use. End users typically tend to do little to configure these devices or perform any additional configuration to better secure themselves, simply because they may not know how or because it seems too difficult to configure.

Unfortunately, the default configurations for most home routers leave home networks vulnerable to attacks and offer little security.

With the rise of the Internet of Things, many households now have internet connected home appliances and devices such as Cameras, TVs, Home Automation, Refrigerators, and Entertainment Systems. These devices connect to the internet via the preconfigured home routers, and thus can be easily exposed to the threats of the Internet. Having a home router that is not well configured, grants the attacker the opportunity to take control of the connected devices in the households, and perform malicious actions that tend to either disrupt our way of life, or expose our privacy.

This document provides guidelines on how to better secure the home router and minimize the attack surface associated with the home routers. The scope of this document is applicable to all residential/SOHO/SMB that have an ISP supplied home router.

3 Audience

Homes and Small Office owners based in the state of Qatar, and personnel installing new routers for homes and small offices.

4 Understand the Risk

The default configurations of most home routers offer little security. They are accessible from the internet, easily discoverable, vulnerable due to misconfiguration, and usually powered-on at all times. This combination provides the attacker with an attack surface that is perfect to exploit.

Moreover, malwares are exploiting default configurations to automatically propagate and replicate all over the internet. These infected devices are then configured as part of a botnet and are used to facilitate malicious cyber activity that transgresses borders.

5 Guidelines

The following is a non-exhaustive list of steps that a user can take in improving home routers security reducing the probability of internal networks being compromised by malicious actor:

1- **Change the default WiFi SSID**: The SSID (Service Set Identifier) is the name of the wireless network that is associated with your device. It is the name you see when trying to connect to a wireless network on your device. Out-of-the-box, the home router has a default manufacturer set SSID which identifies the make and model of the actual device. This grants the attacker with the information needed to identify any vulnerability associated with your home router.
   a. **Set a generic SSID (Home, office, etc**…) that doesn't identify the owner of the device. An SSID that broadcasts the name of a high profile household or a company is more attractive to attackers than a generic name.

2- **Encrypt wireless traffic using WPA2-AES:** WPA2-AES is the most secure option to use to protect attackers from viewing your internet traffic. Generally, a secured network can be identified by a lock symbol next to the WiFi name, and requires a password to connect to.

3- **Set a complex WPA2-AES password:** Use a complex password when setting a WPA2-AES password, and make sure to change it regularly.
   Choose a password that is:

   a. Has letters, numbers, and symbols.
   b. Use capital and lower casing
   c. Longer than 8 characters.

4- Change default router login username and password: Manufacturers set default usernames and passwords to the devices to provide user access to the routers. These usernames and passwords often have administrative privileges and are usually left unchanged after the initial setup. Leaving the default usernames and passwords grants the attacker an easy way into your network. They should be immediately changed after installation.

5- Turn off your router when not in use: While it may be impractical to turn the routers on and off every time you need to use the internet, consider switching the router off when traveling or not in use for extended periods of time.

6- Disable UPnP. Enable this option only in case you specifically need UPnP.

7- Disable FTP. Enable this option only in case you specially need FTP.

8- **Enable router firewall:** Ensure that the firewall feature is enabled on your router and configured to allow authorized users only access to the network, enabling this feature will

facilitate in blocking traffic from home appliances outside the home network as well as stopping unwanted traffic to home network.

9- **Enable logging:** Enable logging in your router and review the logs periodically for any anomaly. The logs can also come handy to aid in the investigation in case of any attack.

Keep in mind that this is only a list of suggested steps that can be taken to potentially secure your router. For further assistance on any technical issue, kindly refer back to your ISP (Internet Service Provider).

6 Incident Reporting

Report any suspicious activity or unusual behavior from your home machines to Q-CERT. Q-CERT provides Public Incident Handing service to Home Internet users through the following channels:

Hotline Numbers: +974 – 44995444 / +974 – 44995445

Website : http://call.qcert.org/

For more information about Public Incident Handling Service and to download free tools, please the following Q-CERT Portal: http://call.qcert.org/