وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

Security Guidelines for VPN Services

Version: 1.0

Author: Cyber Security Policy and Standards

Document Classification: Public

Published Date: march 2020

Document History			
Version	Date	Description	Comments
1.0	March 2020	Ver 1.0 Final Document to be Published	

Table of Contents

Legal Mandate(s)

Cabinet decision No. (26) for the year 2018 of the establishment of Cyber Security Sector within the Ministry of Transport & Communications , and 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 (2) of the Cabinet decision No. 926) of the year 2018 and 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.

Introduction

Organizations today work 24x7 and 365 days a year. Availability and accessibility of systems is critical to a business. There is an imperative need for the employees to have access to the systems when they are on the road, when meeting clients, when at home or even when travelling abroad. Organizations need to come up with viable **secure mechanisms** to make the systems accessible for its employees.

A generally accepted solution is to use VPN services to connect to enterprise systems from remote locations.

This document looks at some of the risks posed by the use of VPN technologies; and how to mitigate them to provide secure access to its employees when they access enterprise systems from untrusted networks.

Objective

The objective of this guideline is to help organizations understand the potential information security risks associated with the use of VPN services and identify suitable controls to mitigate or avoid such risks.

Scope and Audience

Any organization or individual that uses VPN to access enterprise systems.

Understand the Risks

VPNs allow you to connect a remote system to your enterprise system. The remote system could be a company owned and managed device or an employee owned unmanaged home device or worse a public terminal at an internet kiosk, business lounge or an airport. These devices will connect through a home broadband connection, ISP Data services, public wi-fi or guest wireless networks, in all cases untrusted networks so to say.

As such you are increasing the threat attack surface for your systems unless these threats are suitably controlled and the risks mitigated.

The key risks that the organizations faces include:

1. Loss of personal and confidential data.
2. Denial-of-service attacks and preventing the use of operational systems.
3. Corruption of data leading to loss of integrity.
4. Financial frauds
5. Reputational damage caused as the consequence of any of these risks occurring

Evolving Threats

The following are some of the leading threats faced from misconfigured or improperly secured VPN services

WiFi-based attacks: Unless secured adequately, traditional WiFi systems are vulnerable and malicious actors (This could be insiders such as guests using the wi-fi facilities or hackers, cyber criminals etc.) could use them to breach into corporate systems or fellow users.

DDoS and botnet attacks: Distributed-denial-of-service attacks have grown in popularity to carry out a range of malware injection activities. Within such attacks, hackers utilize botnets of compromised networks to flood critical systems with traffic, which results in a crash of the platform. Attackers may also ask for a ransom amount from the authorities to prevent disruption of such critical systems.

Data Leakage: These are attacks where malicious actor gain access to your systems and stay there as much as possible and try to identify and exfiltrate critical data outside the organization. The data includes business data as well as guests information (personal / financial (credit cards) etc.)

Phishing: These are attacks where an attacker poses as a legitimate institution or an individual to lure the target into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

Guidelines

24x7 work, 365 days a year is increasingly becoming a business imperative. The need to ensure that the information systems are available and accessible at all times is a necessity and not a luxury anymore.

Nevertheless, it is very important to ensure that there are no shortcuts; organizations should ensure that the remote access provided to its employees and / or supply chain is secure and adheres to best practices.

Organizations should ensure a security by design approach to bake in security in to its enterprise systems. On a minimum, consider the following factors:

1. Access Surface: Access to information assets should be restricted to limited and regulated communication channels only. Further, only make available information that is required. Hide all other information as much as possible reinforcing the concept of “Security by Obscurity”.
2. Defense in Depth: Protect the Information asset at multiple levels and points using multiple techniques and technology. The security of the system should be assessed against the least secured asset in the system (weakest link).
3. Adequate Protection: The security controls chosen should be adequate and appropriate based on the Risk profile of the organization and the risk to the asset itself as well as the value of the asset itself.

The guidelines below recommend the best practices that organizations should follow. The document complements the National Information Assurance Policy V2.0

Authentication:

1. Use Multifactor Authentication (MFA) to protect against any password breach.
2. In case if it is not feasible to implement MFA, organizations should use Username and Passwords with additional measures such as IP Source whitelisting, MAC Address filtering etc.

3. Passwords should comply with corporate password policy. On a minimum use passwords that are easy to remember and hard to guess e.g. passphrases and change passwords at regular intervals.
4. Special attention should be placed on Administrative or Privileged accounts.

Authorization:

1. Access to enterprise systems should be provided based on the least privileges and Need to Know and a Need to Have basis.
2. Limit the number of systems or targeted hosts that will be accessible to remote users.
3. Organizations shall gradually publish enterprise applications (based on its criticality/priority and subject to due diligence) on the intranet to be accessed over the VPN.
4. Limit number of protocols and services used by remote users. For example, allow only secure protocols such as Https. Restrict the use of Remote Desktop, or SMB to access share folders unless there is a business necessity.
5. For Remote Desktops, organizations should explore options such as:
    a. Use Remote Desktop Gateways. All Remote Desktops requests should be gated through a central server.
    b. Tunnel your Remote Desktop: If using an RD Gateway is not feasible, you can add an extra layer of authentication and encryption by tunneling your Remote Desktop sessions through IPSec or SSH.
    c. Change the listening port for Remote Desktop: Security by Obfuscation, changing the listening port can protect against hackers who are scanning your network.

Availability:

1. Protect against single point of failures, using redundant elements and high availability concepts.
2. Ensure that sufficient bandwidth is available to ensure remote access users are able to access corporate services without any latency in the services
3. Implement controls to protect against denial of services (DOS/DDOS) attacks.
4. Use applications such as Video Conferencing judiciously (on a need to have basis) to conserve bandwidth.
5. Ensure and monitor service level agreements with your internet service provider.

Integrity:

1. Ensure the integrity of deployed VPN solution by ensuring that the software and hardware is updated with the latest fixes and patches.
2. Ensure that the remote user's computer is:
    a. Managed and restricted as per the corporate information security policy.
    b. Up to date with the latest fixes and patches.
    c. Hardened as per the company policy and is configured with an Endpoint protection system.
3. In case you allow the remote users to use their personal devices such as laptops and tablets, make sure that they adhere to a minimum acceptable configuration. This should include an acceptable Operating system (with a minimum patch level) and an endpoint protection system with latest patches and updates. You may also refer to the BYOD Policy for additional guidance.
4. Access to enterprise systems should be restricted from public Wi-Fi systems.
5. Disallow split tunneling unless suitable controls are in place and allow only one connection at a time.

6. Disconnect VPNs from the network after a pre-defined period of inactivity and user needs to logon again to reconnect to the network.

Confidentiality:

1. Ensure that all Internet service request from Internet browsing and DNS (Domain Name Services) are routed through the corporate internet connection and logged.
2. Secure the configuration of the VPN Servers.
3. A copy of updated and tested configuration should be stored in a secure location to be used in case of a disaster.

IPV6 (IPv6 Provider Edge (6PE) and IPv6 VPN Provider Edge (6VPE))

1. It is recommended to address space, routing and traffic separation with the help of VRF (only applicable to 6VPE).
2. Hide the IPv4 core, which helps to remove all attacks against P-routers.
3. Secure the routing protocol between customer edge (CE) and provider edge (PE). In the case of 6PE and 6VPE, link-local addresses can be used and as these addresses cannot be reached from outside of the link.

Logging and Monitoring

1. Define and implement a Logging and Monitoring process in line with the NIA Policy.
2. Ensure all remote users from VPN connection accessing the internal and external applications are logged.
3. Organizations should ensure that adequate events are logged necessary to identify and assist in investigation of security incidents. The system should be able to trace back date, time, usernames, IPs, Services, and Applications, that have been used by remote users.
4. Maintain logs for a minimum of 120 day in line with Cyber Crime Law.
5. Monitor the security logs on a 24x7 basis, at least for the critical systems.
6. It is recommended to correlate logs from various systems to get a holistic view of the operations.
7. Ensure that the Remote systems and the VPN systems are synchronized with the enterprise NTP server

Incident Reporting and Management

1. Establish mechanisms for users and employees to report information security incidents in a responsible manner.