وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

Cyber Security Guidelines for Small Datacenter

"A guidance document for small datacenters and dedicated computer rooms"

Version: 1.1

Author: Cyber Security Policy and Standards

Document Classification: Public

Published Date: June 2018

Document History:

Version	Description	Date
1.0	Published V1.0 document	February 2014
1.1	Branding Change (ICT to MOTC)	June 2018

Table of Contents

Glossary

AC	-	Air Conditioning
DC	-	Datacenter
CCTV	-	Closed-Circuit Television
HVAC	-	Heating, Ventilation, and Air Conditioning
UPS	-	Uninterruptible Power Supply

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.

Introduction

Data Centre is a dedicated facility that houses the information-processing infrastructure specifically the servers, storage equipment and the core network infrastructure. Considering the criticality of these equipment (24x7 operations) and its operating requirements (Requirements such as cooling, ambient temperature, etc.), special care needs to be taken to ensure that the optimum environment exists for it operations.

A number of factors need to be considered in setting up such a Data Centre. This manual gives a high level overview of the factors that need to be considered in setting up and managing a small data center and dedicated computer rooms.

Although the document maps to a number of controls specified in the National Information Assurance (NIA) Policy, this is still a simplified document aimed at small and not so critical Data centers. Businesses / organizations are advised to specifically refer to NIA Policy and the relevant Data center standards such as TIA 42 for complex / critical Data centers.

Objective

The objective of this guideline is to provide security guidance to our stakeholders while choosing open source software solutions. It will help organizations to understand and evaluate the security risk associated with using Open-Source Software and how to mitigate it.

Scope

Datacenter in this document specifically refers to small data centers or dedicated computer rooms setup in small or medium offices / businesses. There may be smaller floor level/area wise switches that may be placed in switching closets. Such switching closets will also require most of the controls mentioned in this document.

Key Consideration for Data Center

Data center is the nerve center of IT computing infrastructure. Proper thought and consideration must be done while designing your Data center. This is not only to meet the space requirements but also to ensure an ambient environment and the necessary security to protect the critical IT infrastructure that resides within.

Following are some of the key considerations:

- ✓ Space considerations
- ✓ Structural loading considerations
- ✓ Power and Cooling considerations
- ✓ Redundancy / Backup considerations
- ✓ Green Data Center considerations
- ✓ Security and Operational considerations

A. Data Center Design

Capacity Planning

Capacity planning in the data center is about making sure that you have adequate computing power and required infrastructure (physical space, cooling, power etc.) to handle the current and near future needs of the organization / business.

Design Data centers and support infrastructure to be scalable and be able accommodate future growth with little or no disruption to services.

Key consideration while doing capacity planning for Data center:

1. **Analyze Current Capacity**
   Determine the current capacity of systems to analyze how they are meeting the needs of the users.
2. **Determine Service Level Requirements**
   Determine the business requirements and the level of service expected and or committed by the IT department
3. **Planning for the Future**
   Finally, using forecasts of future business activity, determine future system requirements. Implementing the required changes in system configuration will ensure that sufficient capacity will be available to maintain service levels, even as circumstances change in the future.

Location / Space

- The location of the datacenter should be inconspicuous so as not to attract undue attention.
- Do not locate the Datacenter directly below water pipelines (eg: bathrooms, drainage piping, AC water collectors, etc.) as it has the risk of water leaking through the walls/ceiling.
- Datacenter should not have outside facing windows. (Outside facing windows have the risk of easier break-ins and trouble in controlling datacenter temperature).
- Walls surrounding the information processing facility should contain or block fire from spreading. The surrounding walls should have at least a two-hour fire resistance rating.
- Consider the number of racks (servers, network (active and passive) equipment), along with the space required for technical equipment while calculating the floor area required. The area should be able to meet requirements of near future as well.
- If possible, Servers/equipment with different data-classification levels should be segregated into different zone to restrict access to it.
    - Segregate utility services (UPS, AC Package Units, fire protections equipment (FM200)), network components and application servers from each other.
    - It is advisable to have a separate Vendor service area for unpacking and assembly of goods.

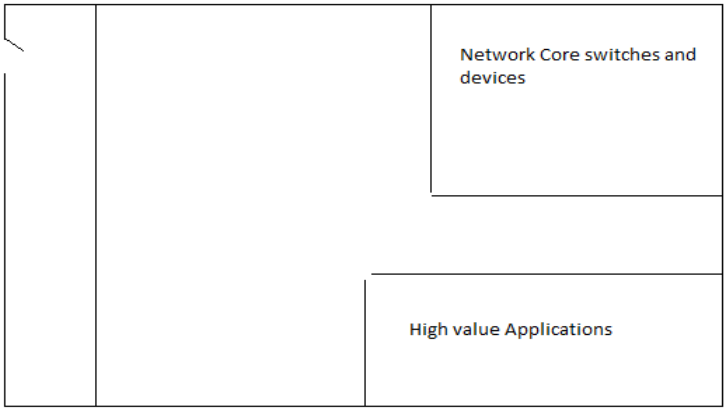

Figure 1: basic data center topology

- Adequately house all electrical equipment such as batteries for UPS, Diesel Generators, Fuel drums etc. in consideration of their hazardous nature.

Structural Strength

- Consider the structural strength of the building and the weight that the building and the floor can take especially if the data center is going to reside on a higher floor (Any floor above second).

Flooring

- The Data center with a raised floor provides a hidden void for the passage of mechanical, electrical and data services. However, such flooring needs to be strong enough and reinforced with additional structural support to take the load of heavy equipment installed in the Data center.
- A lot of Data center also make use of overhead trays for routing mechanical, electrical and data services instead of raised floors.
- Air circulation / cooling is another factor that could affect the decision on usage of raised floors.
- A properly designed raised floor helps in improving the structural strength and load bearing capacity of the Data center floor.

Power Regulators, UPS and Diesel Generators

- Calculate the power ratings needed for the datacenter taking in to consideration the future needs including the 20% power safety factor and the current capacity available for consumption. (There might be restrictions on the amount of power available (in terms of current / amperage) in the office building). An over usage may run the risk of causing electric fires. Refer Appendix A for example.
- Any new hardware addition in the Data Center shall mandate the re-evaluation of power requirements.

- Design the power system to ensure it addresses risks such as Black outs, Brown outs, spikes, surges and Electromagnetic interference.
    - Use Power regulators to regulate power, prevent spikes or brown outs in the power, and thereby protect the equipment.
    - Choose a UPS with sufficient backup power enough to shut down the systems gracefully in an emergency / power failure in cases where the offices / business cannot accommodate a backup diesel generator
    - Diesel Generator (if viable as an option) will provide an effective control against long outages.
- Store the batteries in a suitable controlled and secured environment as per the manufacturer's instructions.
    - High temperature will reduce the life of the battery.
    - High humidity can cause the battery to erode faster.
- Install the generators in a suitably controlled and secured location.
    - Ensure that there is no risk of flooding / water accumulation.
    - Suitable ventilation exists and the area is accessible for regular maintenance and operation.

AC/HVAC

- Design Datacenter and arrange racks in a manner to facilitate circulation of hot / cold air. Consider factors such as raised flooring / false ceilings if they exist.
- Control and monitor the temperature in the datacenter to be between 18oC and 22oC.
- Maintain humidity in the datacenter between 22% and 30%. (if the air is too dry it will cause static electricity generation and if the air is too humid it will cause condensation and lead to corrosion)
- Disable/Close building AC/HVAC Air supply and return vent in Data Center area.

Fire Suppression System

- The datacenter should be suitable equipped with fire protection systems. This includes
    - Detection:
        - Fire (Heat) detectors, Flame detectors and / or smoke detectors.
        - Fire Alarm system
    - Protection:
        - Automated fire suppression systems must be in place.
- The fire protection systems shall take into consideration the following factors:
    - Place fire/smoke detectors at appropriate locations including areas below and above the false ceilings, and areas below the raised floor.
    - Avoid usage of water sprinklers (Dry/wet) within datacenters and disable preinstalled water sprinklers in case it's provided by building owner
    - Configure FM-200 installation with an appropriate time delay to allow the human occupants of the room to exit the datacenter before it dispenses.

Water / Leakage Detectors

- Install water / leakage detectors near the drains and appropriate locations such as below the false ceiling and raised floor areas.

Cabling

- Follow best practices associated with implementation and maintenance of cabling system.
- Label the cables clearly and have identification tags attached in compliance to the classification scheme used in the organization.
- Route power and data (copper) cables in separate trays as per the best practices and manufacturer instructions
- Place wirings, cables in fire resistant electrical panels and conduit to reduce the risk of electrical fire.

Green Data Center

- Use a green approach while designing the Data center to ensure that the Data center is environmentally friendly and resource-efficient throughout its life cycle from construction to demolition.
- Going green benefits an organization in a number of ways:
    - It results in tangible savings through reduced power consumption, greater durability and economical usage of natural resources.
    - Compliance to evolving Green standards

Physical security

- Implement a multi-layer security based on the criticality of the Data center to the organization.
- All entry points into the Data center are secured and not by passable. Perimeter walls should run from floor to ceilings.
- All equipment in the data center should also have security locks or equivalent safety measures to control physical access to them.
- Entry and exit into the datacenter must be controlled and monitored. Depending on the level of risk, the management may decide to use tools such as physical security guards, card readers, man traps, video camera, and biometric devices.
- Restrict access to the data center and allow only authorized personnel to enter the areas that they are required to work in or visit.
- Maintain physical access logs for both staff and visitors.
- Activities in critical operational areas of the data center should also be monitored and recorded. If possible, use motion sensitive cameras and/or passive infrared sensor (PIR Sensor) to record activity taking place within the datacenter.
- In case of usage of temporary walls/curtains, attention must be placed for air distribution, Pathways, etc..
- The perimeter wall shall be sufficiently strong.
- Adequately secure all electrical equipment such as batteries for UPS, Diesel Generators, Fuel drums etc. to prevent any accidents / mishap or sabotage.

General Considerations

- Ensure adequate lighting in the datacenter.
- Do not use the Datacenter or the switching closets as storage or dumping area.
- Keep the Datacenters clean and dust free. Do not allow staff / visitors to eat / drink inside the datacenter.
- It might be prudent for Data centers that do not have a generator facility to have an Emergency Shutdown or Emergency Power Off button to quickly shutdown the power to Data Center. However care should be taken, including the following steps:
    - Place the Emergency shutdown buttons/switch close to the exit.
    - It should be suitable encased / protected to prevent accidental activation.
    - Place clear signage around the switch to alert staff / visitors.
    - Configure / Integrate servers and network components to allow for such a setup.

Consider due diligence in determining the devices that should be connected to the emergency shutdown switch.

B. Data Center Operations

Data Center Machine Room Etiquette

All persons working / visiting a Data center should endeavor to maintain a clean and efficient environment. This may include but is not limited to:

- Keep all work areas clean and free of debris. Upon completion of any work in the room, staff performing the work should ensure they have left the area as clean as it was before their work began.
- Keep all rack enclosures neat and free of manuals, diskettes, cables, etc. Keep the doors on all racks closed at all times.
- Never string cables outside of rack enclosures. Cabling between rack enclosures of adjacent racks may be permitted provided sufficient pass-through chassis are in place.
- Do not eat or drink at any time within the Data center.

Operational Controls

- ***Monitoring:***
    - Monitor regularly control logs, alerts etc. to identify any potential threats and or breaches to the system.
    - Automate systems to alert concerned authorities in case of emergencies such as power failure, HVAC failure, fire alarm etc.
    - Monitor health of the systems (Servers / Network infrastructure) to identify any bottlenecks in delivery of agreed service levels. The inputs shall be used for future capacity planning exercises.
- ***Audit of Processes:***

- Conduct regular audit through Internal Audit department / External audit to ensure compliance to documented processes. This includes processes related to physical security, capacity planning, change control, security monitoring etc.

- ***Regular Inspection of Fire detection and control equipment:***
  - To ensure that all fire detection systems comply with building codes, the civil defence department should inspect the system and facilities annually.
  - In addition, the civil defence department should be notified of the location of the computer room, so it can be prepared with appropriate equipment in case of emergencies.

- ***Regular Inspection and maintenance of control systems:***
  - The facilities team along with the equipment vendor shall regularly check and maintain all electrical equipment and control systems to ensure their worthiness.

- ***Cleaning***
  - A member of IT team should supervise the cleaning of Data Center.
  - Train the cleaning staff in order to avoid accidents and or mishandling of critical systems in the Data center.
  - Draw power for cleaning equipment from a source outside the Data center to avoid spikes.

- ***Training:***
  - Provide training to staff handling mechanical, electrical and control systems.
  - Ensure other operational staff such as security guards, cleaners etc. are also provided awareness and process trainings.

- ***Documented and Tested Emergency Evacuation Plans:***
  - Evacuation plans should emphasize human safety, but should not leave IPFs physically unsecured. Procedures should exist for a controlled shutdown of the Data center in an emergency.
  - On a minimum an annual drill shall be conducted, if required with the civil defence authorities to ensure that people are trained and are aware of things to do in case of an emergency.

Appendix A

Sample Electrical Power Load Calculation

While considering the Power required for a datacenter the following categories of electric consumption must be considered:

-Critical load

Include max power drawn by servers, routers, storage devices, telecom devices, security systems, fire & monitoring systems, etc.

-Future load

Excess power capacity as contingency for growth can be considered at 20% to 30% of currently critical load.

-Peak power multiplier

This factor is to ensure that if all the devices draw power simultaneously, it will not trip the safety system. Usually a 1.05 times of critical load is considered.

-UPS/Battery inefficiency

Battery charging and UPS devices also consume some amount of power. This can be upto 32% of critical load.

-Lighting load

Lighting needed in the datacenter at about 2watts/sq.ft.

-Cooling load

Depending on the device used, cooling devices may need power upto 70% of critical load.

Formula for calculation

Peak power drawn= Critical load * Future load * Peak power

Total utility estimate for datacenter=(Peak power drawn + Total UPS/Battery inefficiency + Lighting + Cooling load) * 125%

The generator needed for supporting this datacenter will be around 30% to 55% of the Total utility estimate.