ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 10, Issue 3, pp: (98-105), Month: July - September 2022, Available at: www.researchpublish.com

Disaster Recovery Plan for Network Service Provider

Sultan Z Al-Khaldi

DOI: https://doi.org/10.5281/zenodo.7116002

Published Date: 27-September-2022

Abstract: **We cannot prevent accident or outages in business even with low probability risk, major outages could destroy a company, if it does not have an effective business continuity plan or disaster recovery plan. It may impact its reputation severely. This paper discusses the importance of such plan with the risk and cost analysis related to disaster recovery. The design of network should be tolerance for failure and consider redundancy for devices which has high impact on the operations. The network team should practice hardening the network equipment's by disabling unsecure protocols and fix vulnerabilities in timely manner. In addition, design a portable communication room that can be used in case of major outage take place. Also define the location of these portables that will help in fast recovery of services. Finally discuss the importance of conducting regular drills and assure the effectiveness of disaster recovery plan.**

Keywords: **Disaster recovery plan, risk analysis, IT networking, business continuity.**

1. INTRODUCTION

The world is advancing at a rapid pace. Since the start of simple machines that helped human beings in daily tasks, humanity has progressed rapidly towards a bright future. The technological advancements made today have proven to be significantly useful in making life easier. The advancements made in every field of science and technology owe their success to the use and implementation of information and communication systems. The use of information and communication systems has made the world into a global village, making it significantly easy and simple to communicate with anyone across the globe in a matter of seconds. The use and implementation of information and communication technology have applications in every field and domain of life, from medicine, engineering, to infrastructure and architecture along with avionics and aviation.

The innovation in the field of information and communication technology has made it possible for scientists and researchers to explore new dimensions to improve the communication systems responsible for transmitting data from one place to another. The use of networking is embedded in the foundations of communication. Without the use of network technology, communication between large enterprises transferring and transmitting data over multiple domains would become impossible. Information technology has become an integral part of human resource management and operational functions. Information technology plays a critical role in the configuration and storage of information by the use of software networks, hardware, and other devices. Business enterprises all over the world rely on the use of networking and information communication. Initially from wired networks technology, the innovation in the field of networking has opened new domains in wireless networks. Computer networks have significant advantages in terms of communication and transfer of data.

The study being conducted will cover various detailed aspects of network communication, information systems, outages at the network level and their effects, recovery plan and process from outages on different levels of the networks and its effects on the information and communication system.

It would be a wise to investigate all the risks that may affect the company operations, set a plan to prevent the risks or lower the probability of those risks and minimize their impacts. In addition, to have a solid plan to recover the operations if any

incident take place. This is what is called disaster recovery and business continuity plan. Abqiq successful story is an example of a powerful disaster recovery and business continuity plan.

A. Problem Statement

This report will cover the problems faced at the network level in case of an outage caused by any reason stated, the effect of the outage on the IT Company, recovery, and management plans in case of an outage or an unauthorized access attempt. Following the recovery plan, the IT Company can ensure highly reliable services for the customers without having any kind of long interruption caused by outages or any other reason. Assuring that the disaster recovery plan is reliable and up-to-date, the risk can be thoroughly analysed, the analysis of the cost of the impact along with the implementation of the recovery plan and establishment of different sets of security and protection protocols for the reduction of the probability of any impact is critically important to ensure that the company continues to provide its clients with unparalleled services.

2. LITERATURE REVIEW

The literature review section covers the vulnerabilities to a network system along with recovery plans.

A research titled "Scalable, Graph-Based Network Vulnerability Analysis" discussed how to handle vulnerabilities. Indeed, even very much controlled organizations are defenceless against cyber-attack. Ongoing work in network security has zeroed in on the way that mixtures of exploits are the normal means by which an aggressor breaks into an organization. Scientists have proposed an assortment of chart-based calculations to create assault trees (or diagrams). Structure addresses generally potential groupings of exploits, where some random endeavor can take benefit of the entrance accomplished by earlier endeavors in its chain, and the last adventure in the chain accomplishes the attacker's objective. The latest methodology in this profession utilizes an adjusted adaptation of the model checker NuSMV as an amazing derivation motor for fastening together organization takes advantage of, addressing assault charts and recognizing negligible arrangements of exploits [1].

A second one titled "Using model checking to analyze network vulnerabilities" discussed the risk of network vulnerabilities. Networks that are considerably well configured and administrated are prone to vulnerabilities and attacks carried out by cybercriminals. Various studies carried out by researchers in the domain of network security and protection show that the majority of the current tools designed and developed address the vulnerabilities in the network designed in the context of a single host. The vulnerabilities in a network designed to configure multiple hosts are addressed by test cases, attack scenarios, which are generated and designed by a model checker.

A third research titled "Research on Linkage Model of Network Resource Survey and Vulnerability Detection in Power Information System". The research carried out in this study analyzes the challenges and difficulties of power information systems along with the management and network resource survey. The vulnerabilities in the specified domain of the power information systems and associated networks are highlighted in this paper. A vulnerability detection system is designed and developed considering the key elements of vulnerabilities in the power information systems. The vulnerability detection framework comprises three modules with the process of associated vulnerabilities in terms of networks survey and detection linkage is proposed. The research also highlights the implementation technologies associated with the main function attributed to each specified module.[10]

Another paper discussed the vulnerability fixes for local networks. Vulnerabilities arise at different levels in the networking domain leading to exploits and cyber-attacks. The study carried out in this research covers the identification, recovery, and reporting of the network vulnerabilities and loopholes found and identified in the intranet domain. In the terms of cyber security, significant importance is given to addressing the security vulnerabilities for protection against cybercriminals, who can gain unauthorized access through open access points. The system proposed in this research is designed and developed to critically assist the Network Administrator Linux/ Windows operating system users. The tool developed and proposed is designed to detect the vulnerabilities at both the physical and logical level of the ports.

Finally a paper titled "Evaluation of Network Risk Using Attack Graph-Based Security Metrics". As the advancements in the field of networking occur with every passing day, new vulnerabilities are also found in the networks opening multiple dimensions for cybercriminals to exploit and carry out a cyber-attack of different vectors. The approach taken in this paper assesses the risks and vulnerabilities in a network by using attack graphs to determine how the attacker can exploit the security and compromise the network at different layers. The attack graph generated is by Multihost Multistage Vulnerability Analysis (MulVAL) tool. Two security metrics are taken into consideration, exploitability metric, and impact metric. These security metrics analyse and assess the risks and vulnerabilities associated with the network.[8]

3. METHODOLOGY

Considering the problem statement explained in detail, an IT company relying on the extensive and critical use of networks for communication and data transfer may face significant problems. In which outage may affect different vectors and the outage may cause by design issue or other reasons.

The methodology section of this paper will address the response plans that should be taken up and adapted by an IT company in case of an outage. The methodology will cover the disaster recovery plan in terms of the network domain while presenting different solutions to the problem statement.

1- Problem statement shows the important of disaster recovery plan.

2- Causes of network outages.

3- Design consideration such as redundancy and tolerance to network outages.

4- Hardening the network by applying compliance configuration and assure no vulnerability affecting current version.

5- Design portable communication room equipped by network equipment's that can restore a major network outages. Cost estimation of such communication room.

6- Define the proper location for the portable commination room, using coverage distance and population density.

7- Risk analysis and incident classification.

8- Set a guideline how to handle a cyber-attack.

9- Define who will lead the incident recovery activity? And what is his/her role?

10- Discuss the importance of drill to improve the incident response plan.

4. DISCUSSION AND RESULTS

A. Potential Reasons for Network Outages

Network outages can cause significant problems in terms of productivity, lost revenue, and damage to critical infrastructure. Following potential reasons for network downtime are explained:

- Human Error: Most of the time, a network faces downtime is due to a human error. For people who do not know the information relevant to the networks, written procedures including checklists are crucial to avoid any accident.
- Understaffed IT departments: The IT departments must have a trained team that is responsible for keeping the IT Company's network, servers, and applications in check is significantly important to keep the red flags in check.
- Old Software and Hardware: If an IT company is using outdated software and hardware, this can lead to many problems eventually causing an outage.
- Bugs and Vulnerabilities, Cyber Attacks: As previously mentioned in the literature review section, vulnerabilities in different layers of the network can lead to cyber-attacks carried out by hackers and cybercriminals.
- Natural Disasters: Natural disasters are the elements of networks outage that can cause significant damage not just to the software but also damages to the key infrastructure and loss of property and hardware. [2].

B. Design Consideration

1) Area Defined Network Resilience

Network resilience is defined as the robust ability of a network to maintain its services in the event of damages, faults, and challenges. As network outages and challenges are unavoidable, the resilience of a network should be considered one of the key elements in the strength of a network communication system.

Survivability is also defined as the ability of a network to respond to both physical and logical faults by redirecting the traffic to routes that are not affected and are providing operational services. The scope of survivability extends further than the narrative and objective of fault tolerance revolving around interrelated failures of networks that are unbounded. Apart from fault tolerance, another key element in the resilience of the network is redundancy. Redundancy pertains to the ability

incorporated in a network that assures the system does not get affected by the same fault multiple times under similar correlated failures.

- Fault tolerance: As previously mentioned, fault tolerance is the capability of a system to endure the damages done resulting from events other than the failure of services. The concept of fault tolerance employs the element of redundancy to avoid the failure of a system from the same multiple correlated failures. Although applying two different approaches, fault tolerance is not considered a sufficient recovery option for multiple correlated failures.

- Disruption tolerance: Disruption tolerance is defined as the ability of a network to tolerate the interruption that occurred in the communication or connectivity between different components of a network. The connectivity and communication are determined by the path characteristic which may be affected due to various challenges including weak channel connectivity, mobility of nodes, latency, and power challenges.

2) Traffic Tolerance

Traffic tolerance refers to the capability of a system to tolerate and endure unpredictable and spontaneous traffic loads. Given the advancements in network technology, an unreasonable load of traffic can be generated within a matter of minutes that falls outside the capability of the network bandwidth. This can cause the network to slow down and eventually crash. This usually occurs in the event of a malicious activity carried out such as a DDoS attack.

3) Dependability

The dependability clause in the resilience of networks against prompted or unprompted outages pertains to the quantification of the service reliance comprised of reliability and availability. The reliability and availability fall under the domain of service continuity in a given time frame. Availability stands for the measures in transactional services such as HTTP-Hyper Text Transfer Protocol, which is responsible for performing various operations in a short period.

4) Backing up The System

Reinforcements alone don't comprise a total disaster restoration technique, be that as it may. Other than keeping up with duplicates of your business-basic information in a safe optional area, you have to likewise be trying your restoration techniques routinely. It requires some investment to re-establish information and applications from reinforcement, so it's fundamental to guarantee that the recuperation cycle can be finished rapidly enough to ensure the integrity of your business' tasks. When arranging and testing your restoration systems, you'll need to monitor two significant measurements.

Recovery time objective (RTO): assigns how long your business can make do without admittance to the information or application being referred to. It's a proportion of the most extreme measure of time it can take to re-establish the framework to full working activities.

Recovery point objective (RPO): portrays how much information your business can stand to lose, and in this way directs how often reinforcement duplicates of your information ought to be made.

5. INCIDENT RESPONSE PLAN

IRP a document describe the action need to be taken in case of an outage, could include a classification if service interruption scenarios and a guide line what to do in each case. Could include a reference of time to restore the services, escalation procedures, how to communicate the outages between the restoration team and management or customers.

The monitoring tool should have access to the cost of the services so that when it shows a switch is down it calculate the bills of all services connected to it. The monitoring technicians should be able to generate a report for the total cost for an incident when it take place, it would be better if such report is generated by the NMS. The monitoring technicians should have a report of planned changes with expected impacts of any change. Also non-service impact changes should be reviewed to avoid announcing a false positive incident.

Rule of thumps when suspect the outage is related to change role back and check if the service restored before announcing a major incident. A service provider should list all the services it provide, with a list of all possible scenario of outage, and have a plan how to respond to each failure and what is the resources needed for successful restoration. The document need to be reviewed and updated annually and tested by a drill. Business continuity engineer should conduct un-announced drill and measure the response of all entity involved in the restoration plan. He should compare the results of the drill with the one in the IRP and investigate any deficiency. Observations should be treated seriously and fix them or adjust IRP.

A. Drill is Important

Select a service or location where all services there went down assumption. Need to restore it from zero. A drill could be announced so that everyone know his role in the drill, such drill help in training or practice disaster recovery. Unannounced drill helps in measuring the effectiveness of disaster recovery plan. Such a drill could be initiated by one of the IT department managers. He/she call for a meeting and share a drill plan to be executed in same day. Below points could help in preparing an effective drill pan:

- List all operation depend on it and measure the impact on company operations or income.
- Find alternative to replace such service.
- List resources needed to restore it and how long to execute it
- Is there a plan to restore it in short time with low cost. If not prepare one. If yes execute that plan and observe the execution process.
- Set key measure of successful restoration.

After the drill, conduct a critique meetings discussing the documenting the observations of the drill. Propose solutions and resolve these observations. Lesson learned and train the team to handle major outages.

B. Cyber Attack

Before

1- Classify all data, Doc, or information of the company.

2- Set a guideline how to handle each classification, and who has access to it.

3- Assure the company have tools that can detect/prevent and resources needed to investigate an attack. Have the team trained how to use such tools.

4- All system are backed up, have a plan to rebuilt any system from backup and test it frequently.

5- Regularly check for compliance and have a systematic way to assure all systems are in complaint.

6- Vulnerability: have a plan to check for new vulnerabilities, and assure fixes are applied in timely manner.

After/ during

7- In case a zero day vulnerability or attack detected, follow up with vendor to update detection or prevention system. Assure the fixes patched to all related systems.

8- Report any attack to government law based on the country regulation some in 3 days others within 7 days.

9- The information security manager will lead the incident.

10-To avoid long escalation process and distortion for actions needed during cyber-attack, all others mangers will be isolated from their rules. One highly skillful engineer will lead the action under the department responsibility. This engineer will report to the incident manager.

11-Stop/cancel all changes activity not related to the incident.

12-Part of the team should work on shift to assure a quick response, all action taken should be documented and turned over to the next shift.

6. RISK AND COST ANALYSIS FOR DR PLAN

A. Incident Classification

From risk matrix of the company, cost value, repetition, competitive value and safety were selected to classify the incident to three levels and below example of level 1.

Level 1:

- The cost of affected services is x% of the company revenue.
- Affect a competitive value.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 10, Issue 3, pp: (98-105), Month: July - September 2022, Available at: www.researchpublish.com

- Cyber security attack
- Isolation of a city or large area of it
- Loose of life

B. Risk Analysis

Table I list the possible service impacts with probability of failure and mitigation plan for each.

Table I: RISK MANAGEMENT MATRIX.

Outages	Impact description (risk)	Probability	Mitigation
Switch-A	Local impact	0.9995	Spare part available
Switch-B	Local impact many users	0.9999	Spare part available Redundancy
L2 link	Single user one site	0.999	Fix it, customer should have a backup
L3 link	Single user one site or more	0.999	Fix it, customer should have a backup
Edge router	Uplink for major customers and switches.	Redundancy (0.9999)	Spare part available Redundancy
Core router	Uplink for edges no impact with single failure	Highly redundant (0.9999)	Spare part available Warranty Portable CR
Communication room	All above listed services commonly affected. It may contain local service provider of international		Migrate the service to nearest communication room. Portable CR
Local service provider link	Connection between different service provider customers	Highly redundant	Fix it Highly redundant
International service provider link pass through	Connection to internet	Redundant	Fix it Highly redundant
DNS/NTP	Internet services	If not affected by cyber-attack then probability of failure is zero.	High security design Backup and documented recovery plan
Major customer	Customer leasing its LAN & WAN services		Fix it, customer should have a backup

C. Portable Communication Room

The portable should reach the incident location within acceptable time around 4 hours. The design to have four portables in different location so that it can reach the incident site with acceptable time. I have analysis the location of these trucks based on the distance between the Kingdome cities and based on population density.

500 Km distance:

Table II: Location of portable communication room according to 500Km coverage distance.

Location	Coverage Area
Riyadh	Abqiq- Hafuf- Kharj- Damam- Khober – Buridah- Majmaa- Hafer albatin.
Maddinah	Taif – Jedah- Makah – Hail
Abha	Jizan – Najran – Albaha
Skaka	Quriat – Tabuk –Turaif – Arar

Population density:

Table III. Location of portable communication room according to population.

Location	Population
Riyadh	11 Million Lives less than 400km from it.
Makah/Jeddah	9 Million Lives less than 470km from it.
Dammam	5 Million lives less than 500km from it
Abha	4 Million lives less than 330km from it

Table IV. Cost estimate for portable communication room.

Equipment	Cost	Power	Weight/ dimensions
Switch-A cisco 9200L-48 port	2563 $	600 W	1.73 x 17.5 x 11.3 in 5 kg
Switch-B cisco c9404R	31000 $	3200 W	10.5 x 17.5 x 16.3 in 17 kg
FW- cisco Firepower 4100	22000 $	1100 W	1.75 x 17 x 29.7 in 16 kg
L3 link	-	-	-
Edge router- cisco 4451	16476 $	950 W	3.5 x 17.5 x 18.5 in 13 kg
Core router- cisco 8804	60,000 $	4200 W	17.5 x 17.5 x 33 in 183 kg
RACK	2000 $	-	-
VSAT terminal	5500 $	-	-
Cables	3000 $		-
A/C	3300 $	2000 W	70 kg
Thoria telephone	2500 $	-	-
Generator	5000 $		250 kg
truck	50000 $		-
Total	195339	12050 W	< 1000 kg

7. CONCLUSION

Various approaches to counter the problems faced by network outages are discussed in the report.. The methodology section covers extensive details related to the given scenario in terms of networking and IT. Initially, the potential reasons behind the network outage are highlighted along with the types of attacks that can be carried out at the network level by cybercriminals and attackers. In the next phase of the methodology, the resilience of the network and the recovery processes are discussed in detail along with the component level and layer-level faults that could cause an outage. The recovery process a company should employ in case of the downtime of the IT department and the networks is discussed in detail in the last part of the methodology. The last part of the methodology also highlights the cost and risk analysis for the data recovery plan in case of an impact to the network.

REFERENCES

[1] Ammann, P., Wijesekera, D. & Kaushik, S., 2002. Scalable, graph-based network vulnerability analysis. Proceedings of the 9th ACM conference on Computer and communications security - CCS '02.

[2] David Nizen iGLASS helps IT professionals improve the uptime and health of their IT infrastructure, 2019. 10 reasons for network downtime & what to do about it. 24x7 Outsourced NOC Monitoring Services from iGLASS Networks. Available at: https://www.iglass.net/blog/reasons-for-network-downtime [Accessed November 27, 2021].

[3] GeeksforGeeks, 2020. Importance of Computer Networking. GeeksforGeeks. Available at: https://www.geeksforgeeks.org/importance-of-computer-networking/ [Accessed November 25, 2021].

[4] GeeksforGeeks, 2021. Basic network attacks in Computer Network. GeeksforGeeks. Available at: https://www.geeksforgeeks.org/basic-network-attacks-in-computer-network/ [Accessed November 27, 2021].

[5] Guo, Q. et al., 2019. Research on linkage model of network resource survey and Vulnerability Detection in Power Information System. 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC).

[6] Iloglu, S., & Albert, L. A. (2020). A maximal multiple coverage and network restoration problem for disaster recovery. Operations Research Perspectives, 7, 100132.

[7] Jorrigala, V. (2017). Business Continuity and Disaster Recovery Plan for Information Security.

[8] Lord, N. (2017). Cyber Security Incident Response Planning: Expert Tips. Steps, Testing & More.

[9] Kumar, S. et al., 2016. Evaluation of network risk using attack graph based security metrics. 2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/ CyberSciTech).

[10] Rak, J., 2015. Resilient Routing in communication networks, Cham, Switzerland: Springer.

[11] Ritchey, R.W. & Ammann, P., Using model checking to analyze network vulnerabilities. Proceeding 2000 IEEE Symposium on Security and Privacy. S&P 2000.

[12] Zhang, G., Zhang, F., Zhang, X., Wu, Q., & Meng, K. (2020). A multi-disaster-scenario distributionally robust planning model for enhancing the resilience of distribution systems. International Journal of Electrical Power & Energy Systems, 122, 106161.