DV_T201 RESEARCH DOCUMENT

Erik Conradie 221147

TABLE OF CONTENTS

1 Introduction

This research project offers a thorough roadmap for organising and implementing the IT infrastructure for Glen Hub. This document's goal is to offer insightful observations and suggestions on internal networking, hosting, security precautions, and implementation costs.

As an IT specialist, it is my responsibility to counsel and support Glen Hub as they decide how to best operate and launch their video streaming platform. I will analyse the company's unique needs and objectives and then offer in-depth details and suggestions to help the IT infrastructure be deployed successfully.

2 Internal Network Plan

To provide dependable connectivity throughout the offices, I advise deploying a blend of **Wired and Wireless Networks** for the internal networking design. Consider the following examples of topologies, devices and transmission media:

The topology I recommend is a **Star Topology or Star Network**, in which each device is only linked to a central hub. One of the most common setups for computer networks is this kind of network design. The name of this sort of network comes from the way the devices connected to a central network resemble a star model.

The star topology has a very simple installation as well as an easy way of adding additional devices to the network. This network is very reliable and always has a strong connection, this will allow the network to run with minimal problems.

Transmitting media throughout the network, the offices will need **Ethernet Cables** which is still one of the most popular forms of network connection. Ethernet is used for its reliability, security as well as high speed connections. For the wireless aspect of the network a **WLAN** should be installed. Wireless networks are great for increasing efficiency throughout the company as it leads to improved data communications through remote networking.

Taking a look at the network. I would advise the company to have the following devices:

- **Switches:** This will allow the network to connect to different devices.
- **Servers:** This will grant the company to host the website as well as the streaming services.
- **Wireless Access Points:** For the network and devices to connect wirelessly a WLAN would be recommended.
- **Routers:** To connect to different networks and allow data transmission.

3 Hosting Plan

For scalability and dependability given the anticipated volume of visitors and videos, I suggest a **Cloud-based Hosting** option. You can view your data from everywhere across the globe because it is kept remotely. This is especially useful if you travel a lot for business or if members of your team are spread out across multiple time zones. The scalability is also a major advantage, as our customers grow we can increase the amount of storage for the anticipated data.

Here is a summary of the hosting schedule:

Starting with the cloud provider, I would recommend using **Amazon Web Services**. AWS is based in Southern Africa, as well as it is one of the largest providers for the United States of America. This will help with the connectivity between regions for our users.

I would also recommend the company make use of a **CDN**. This will increase reliability for the servers, as a CDN enables applications to run through any turbulent times. a CDN balances the load of the company network allowing for better performances. Another benefit of using a CDN is the protection against cyber-attacks.

3 Threat Analysis

As a company it is important to be aware of the potential threats that can harm our services. Here are some **Possible Threats** that can occur for streaming companies:

- **Phishing Attacks**

Phishing attacks are social engineering techniques used to deceive users into revealing their personal information, such as passwords, usernames or account details. Attackers impersonate the company through emails, messages or websites to try and trick victims into thinking it’s legitimate entities.

A mitigative measure to decrease the threat is to implement Two-Factor Authentication. Enabling 2FA on the company's system adds an extra layer of security for our users. Even though the details have been compromised, the attacker won’t be able to access the victim’s account.

- **DDOS Attacks**

DDoS attacks typically consist of a significant amount of compromised devices under the command of an attacker, who plans the attack to consume the target's resources, such as bandwidth, processing power, or memory, making it unable to provide service to legitimate users.

A mitigative measure is to implement a DDoS Mitigation Service. These services use specialised content delivery networks (CDNs) or specialist DDoS mitigation services to prevent DDoS attacks. These services ensure that genuine traffic reaches the intended target by collecting and filtering out harmful traffic.

- **Insider Threats**

Insider threats refer to security risks that arise from individuals within our organisation who have authorised access to its systems, data, or resources. These threats can be intentional or unintentional, and they pose a significant risk to the confidentiality, integrity, and availability of sensitive information.

A mitigative measure is to implement some access controls and privilege management. This will ensure that the company’s employees only have access to the data necessary for their assigned roles.

- **Data Breaches**

Data breaches refer to where unauthorised individuals gain access to confidential data within the company. These breaches can occur due to various types of factors such as cyberattacks, system vulnerabilities or social engineering.

A mitigative measure is to implement strong encryption and data protection. This will help keep sensitive data encrypted when compromised. The encryption protocols and algorithms secure data and the company's storage system.

Another measure is to regularly update and patch the networks. Applying security updates to the system helps it to address any known vulnerabilities.

3 Implementation Budget

I can give you an approximate cost and budget for hosting 1,200,000 users in South Africa and 500,000 users in the USA on AWS, including a CDN, based on the information supplied.

It is important to note that there are several aspects that should be considered when hosting a streaming web service on AWS. There are multiple costs associated, including the computing costs, data transfer costs, CDN costs as well as the storage costs. All of these costs are necessary to provide a working service for users.

- **Compute Costs:** Considering an average of $0.20 per hour per instance, assuming a medium-sized instance, the compute cost could be approximately $8,000 per month for South African users and $3,333 per month for users in the USA.
- **Data Transfer Costs:** These costs can vary based on the volume of data transferred. Assuming an average data transfer rate of 10 TB per month for both regions, the cost could range from $1,000 to $2,000 per month.
- **CDN Costs:** Implementing a CDN such as Amazon CloudFront can help improve performance and reduce data transfer costs. The cost would depend

on the data transfer volume and geographical distribution. Assuming an additional $1,000 to $2,000 per month for CDN services.

- **Storage Costs:** Storage costs depend on the amount of video content hosted. Assuming an estimated storage requirement of 1 PB (petabyte) for 500,000 videos, the monthly cost could range from $5,000 to $10,000, depending on the storage service used (e.g Amazon S3).

Based on these estimates, the total monthly budget for hosting the video streaming website on AWS would range from approximately $18,000 to $25,333.

3 Conclusion

In conclusion, this research project provides a roadmap for Glen Hub's IT infrastructure, covering internal networking, hosting, security measures, and implementation costs. As an IT specialist, my goal is to guide and support Glen Hub in deploying their video streaming platform successfully. By analysing their needs and offering detailed recommendations, we aim to establish a robust IT infrastructure that aligns with their objectives.

3 References

Infosec Train. 2023. *Common Security Attacks in the OSI Layer Model*. https://www.infosectrain.com/blog/common-security-attacks-in-the-osi-layer-model/ (15 June 2023)

Cloudflare. *What is web application security?* https://www.cloudflare.com/en-gb/learning/security/what-is-web-application-security/ (15 June 2023)

Elprocus. Star Topology : Working, Features, Diagram, Fault detection & Its Applications. https://www.elprocus.com/star-topology/ (15 June 2023)

Techtarget. Ethernet. https://www.techtarget.com/searchnetworking/definition/Ethernet (15 June 2023)

NiBusinessInfo. Wireless technology. https://www.nibusinessinfo.co.uk/content/pros-and-cons-wireless-networking (15 June 2023)

CDNetworks. 2021. 8 Benefits of Using a CDN and Why Your Business Needs One. https://www.cdnetworks.com/web-performance-blog/cdn-benefits/ (15 June 2023)

Secure Storage Services. Pros and Cons of Cloud Storage. https://www.securestorageservices.co.uk/article/11/pros-and-cons-of-cloud-storage (15 June 2023)