A picture containing icon

Description automatically generated

New Zealand Diploma in System Administration Level 6

# **NET602: Network Services**

# Assessment/Aromatawai - Assessment 1 v2.3

# Case Study

Circle

Description automatically generated with low confidence

|  |  |  |  |
| --- | --- | --- | --- |
|  | Submission | FER1 | FER2 |
| Result | Click or tap here to enter text. | Click or tap here to enter text. | Click or tap here to enter text. |
| Date | Click or tap to enter a date. | Click or tap to enter a date. | Click or tap to enter a date. |
| Assessor’s Signature |  |  |  |

|  |  |
| --- | --- |
| Student Name | Hui (Spark) ZHENG |
| Student ID | AEU3000774 |
| Student Signature | Spark |
| Assessor | Click or tap here to enter text. |

## Task 3.1

In the Task 2.2, the network structure has several potential vulnerabilities:

1. No monitoring and prevention system. The real time attacks could not be detected and responded quickly. This can lead to severe damage before the action is taken. And NZ privacy protection laws require active monitoring and logging, lack of monitoring could result in no-compliance, leading to fines and legal action.
2. No MFA system. If the password of users is leaked, the network will be vulnerable. The attacker can easily access sensitive data and systems, such as domain controller or file server.
3. No proper network segmentation, the data may be accessed between different departments. Once attackers gain access to one part of the network, they can easily jump to other parts of the network, increasing the chances of widespread compromise.
4. Unencrypted data on NAS. The data may be leaked in plaintext. If attacker gain the access to the NAS, unencrypted data can be easily stolen and lead to data breaches. Especially for TechCo Solutions, its data is the most important assets.
5. Only local storage. In the event of hardware failure, natural disasters, or theft, all data stored locally could be permanently lost if there are no backups, and without off-site backups or cloud storage, there is no redundancy. This increases the risk of total data loss in case of an incident.

To Strengthen those potential vulnerabilities, the following security mechanisms should be implemented:

1. IDS/IPS system should be deployed to monitoring and prevent the network. After IDS/IPS system deployed, the network attack will be detected in real time and be blocked or contained. It integrates with Firewall and VPN server to provide comprehensive visibility and protection across the network.
2. MFA system should be deployed to protect the user’s password. MFA requires users to provide two verification factors to get access to network information. MFA integrates with Domain controller, VPN server and other key network services, ensuring that all user access points are secured. MFA significantly reduces the risk of unauthorized access due to compromised credentials, as attacker would need more than just a password to get entry.
3. VLAN should be deployed on the core switch to segment the different departments. VLAN can isolated network segments for each department. VLANs are configured on the core switch and the department switches and each VLAN has its own security policy including access control, firewall rules and monitoring. In case of a breach, the threat is contained within the affected segment, minimizing overall impact.
4. Encrypt the data on NAS to protect the data. Data encryption can be implemented on the NAS through built-in encryption tools. Encrypting data at rest on the NAS ensures that even if the data is accessed by unauthorized users, it cannot be read without the proper decryption keys.
5. Use cloud storage to protect the data. Azura cloud storage is chosen since it is provided by Microsoft and can be integrated easily with Windows server and Windows client OS. Azure cloud storage provides redundancy, ensuring that data can be recovered in case of hardware failure, ransomware attacks, or physical damage to local storage.

No extra hardware is required. For MFA system, the apps could be deployed to user’s mobile phones/tablets.

The extra software is as following:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** |  | **Specification** | **Cost** | **Quantity** | **Justification** |
| Snort ("Snort 3 release,"2024) |  | Version: Snort v3.3.3.0 | Open Source | 1 | Snort is chosen as IDS/IPS Server for it is popularly used free software and to choose free software could save money under the budget. |
| DUO (DUO products. 2024) | Duo Security | latest | $3/Month/User | everyone | DUO provides a fully MFA solution for Domain users to login from computers and it supports MacOS, Windows, Android and IOS. |
| Azure Cloud Storage ("Azure Blob Storage pricing,"2024) | VMS Solution Sdn Bhd | 4TB | $82/Month | 1 | Azure Cloud storage is provided by Microsoft and can be integrated easily with Windows server and Windows client OS. |

## References

1. Snort 3 release. (2024, August 18). Github. https://github.com/snort3/snort3/releases.
2. DUO products. (2024, August 18). DUO Security Ltd. https://duo.com/product
3. Azure Blob Storage pricing. (2024, August 18). https://azure.microsoft.com/en-us/pricing/details/storage/blobs