|  |  |
| --- | --- |
| Assignment 1  ITRI 625 | ENRICO DREYER  31210783 |

Table of Contents

[Introduction 2](#_Toc79404114)

[Various threats to the university’s network 2](#_Toc79404115)

[Controls that are in place 2](#_Toc79404116)

[Firewalls used 2](#_Toc79404117)

[Intrusion detection system 2](#_Toc79404118)

[Security aspects of the email system 2](#_Toc79404119)

[Conclusion 2](#_Toc79404120)

[References 2](#_Toc79404121)

# Introduction

In this report the network security of NWU Vaal in terms of networks will be discussed. The main topics will be the various threats, controls that are in place against the threats, firewalls used, intrusion detection systems that are in place and security aspects in terms of the e-mail system. Throughout the report recommendations will be made when necessary.

# Various threats

According to Charles P. Pfleeger (2015) the four potential types of harm that NWU can experience is *interception*, *modification*, *fabrication* or *interruption*. Although the terminology is a bit different, these types still apply to networks. In terms of *interception*, it is often called wiretapping or eavesdropping, *modification* and *fabrication* is often called integrity failures and *interruption* is often called denial of service.

## Interception

Interception is when an unauthorized party got access to an asset (genesisdatabase, 2010). This party can be a program, a person, or a computing system. Examples include obtaining data in a network (wiretapping). Loss can sometimes be detected easily, but a silent interceptor can leave no trace and no way of detecting interception. The best way to counter interception for NWU is by making use of a strong encryption (spamlaws, 2003).

## Modification

According to genesisdatabase (2010), if a party that is unauthorized not only gains access to data, but also tempers with the data, it is called modification. For example, when someone changes values in the NWU database, or change functionality on efundi. This does not only apply to software, but hardware as well. According to Edwards (2018) some of the ways that NWU can prevent modification is to keep track of changes in the network, make use of atomization and to document network changes.

## Fabrication

This is when an unauthorized party creates a fabrication of fake objects on a system. Examples include when a party inserts spurious transactions in NWU’s network communication system. If skilfully done, they are almost impossible to distinguish from the real thing (genesisdatabase, 2010). According to Rasayely (2019), NWU can make use of certification of data and imposition of supervision on respondents.

## Interruption

This is when an asset becomes unavailable, lost, or unusable. For NWU, this can be malicious destruction of hardware devices, malfunction of an operating system, erasure of data files or programs. According to Murray (2021) what NWU can do to detect interruption is to do constant speed tests, traceroute tests and ping tests.

# Controls that are in place

NWU has network encryption in place to ensure that the network stays as safe as possible, this is in place to counter *interception*. Encryption is one of the most versatile and important tool in terms of network security (Charles P. Pfleeger, 2015). Encryption provides privacy, separation, integrity, and authenticity.

# Firewalls used

A firewall is a device made to filter traffic between an inside or protected network and a less trustworthy network (Charles P. Pfleeger, 2015). There is usually a dedicated device that runs a firewall, as a single point through which traffic is sent, performance is important

# Intrusion detection system

# Security aspects of the email system

# Conclusion

# References

Charles P. Pfleeger, S. L. P., Jonathan Margulies. (2015). *Security in computing*.

Edwards, J. (2018). Managing Network Configuration Changes: Five Best Practices. <https://www.whatsupgold.com/blog/best-practices-in-network-configuration-and-change-management>

genesisdatabase. (2010). *Types of threats | Interception | Interruption | Modification | Fabrication*. <https://genesisdatabase.wordpress.com/2010/12/13/types-of-threats-interception-interruption-modification-fabrication/#:~:text=An%20interception%20means%20that%20some%20unauthorized%20party%20has,or%20wiretapping%20to%20obtain%20data%20in%20a%20network>.

Murray, J. (2021). *How to Check for Internet Interruptions*. <https://www.techwalla.com/articles/how-to-check-for-internet-interruptions>

Rasayely. (2019). Data Fabrication/Falsification… Do Not Ever Do! <https://www.rasayely.com/data-fabrication-falsification-do-not-ever-do/>

spamlaws. (2003). *Types of Wireless Network Attacks: Interception*. <https://www.spamlaws.com/interception-attack.html#:~:text=The%20best%20wireless%20security%20protection%20against%20interception%20exploits,can%20be%20cracked%20in%20under%20one%20minute%27s%20time>.