Netsys Bank

Risk

2022

Evaluatio

Sri Lanka Institute of Information Technology

Group Assignment

IE3052 – Information System Risk Management

Submitted by:

Student Registration Number	Student Name
IT20229320	Tharani Medawatte
	Prasad Sanjaya

Date of submission

28.04.2022

Contents

EXECUTIVE SUMMARY----------3

Penetration Test Results Summary ……..5

FOOTPRINTING AND RECONNAISANCE----------6

Information Gathering - Nmap…….……6

Information gathering – Angry IP Scanner……...9

VULNERABILITY IDENTIFICATION & ANALYSIS, EXPLOITATION AND MITIGATION----------10

Metasploitable system Nessus scan……..……..10

OWASP bwa system Nessus scan ……..11

Exploitation of NFS Exported Share Information Disclosure Vulnerability…….……...12

Exploiting Samba Badlock Vulnerability…….…….....16

CONCLUSION----------21

EXECUTIVE SUMMARY

1.1 Executive Summary

This is the Annual Information Risk Assessment Report of Netsys Bank (Pvt.) for the year 2022 – conducted during the period of 23rd March 2022 to 23rd April. This report contains a comprehensive analysis of existing risks and vulnerabilities of Netsys bank system along with its various subsystems. The risk evaluation aims to summarize the risks which affects and can potentially affect the confidentiality, integrity, and availability of the pre-established assets of the institution that falls under the above-mentioned criteria. The following three most important factors that decide the Information Risk which also influences the confidentiality, integrity and availability of systems and data are evaluated in this report.

- An assessment on threats and vulnerabilities which are regular and man-made
- An evaluation on the cyber security controls that are present and their operational condition.
- The advanced technologies, processes, and the capability of the employees on cyber-hygiene and the general development of the IT security programs.

1.2 Key Issues and Recommendations

TECHNICAL REPORT

1.0 Introduction & Purpose

Netsys Bank (Pvt.) is a private bank which is based in Colombo, Sri Lanka. Netsys Bank provides all banking facilities such as saving, online money transactions, currency exchanges and loan services. With a recent history, Netsys bank is recognized as an upcoming bank in the field of banking in Sri Lanka with its excellent quality of service and with its high customer rating. The bank contains 10 departments with over 400 employees performing duties in conducting banking operations. The bank caters to more than 200,000 customers and maintains more than 500,000 bank accounts. Netsys bank launched their virtual banking platform in April 2020, providing their customers the remote banking opportunity along with online payment gateways to leading apparel, food and supermarket chains for enabling contactless payment options for its customers.

The purpose of this risk assessment is to analyze and identify the vulnerabilities and shortcomings relating to various information assets of Netsys Bank (Pvt.) and to propose suitable mitigation strategies to reduce the current risk levels incorporated with each asset to pre-determine acceptable levels.

1.1 Risk Assessment Methodology

I. Scope

The scope of this risk assessment is limited to 6 critical assets belonging to the HR department, Finance department and the IT department which are identified through a Qualitative Risk Assessment Process. [Appendix A, Section A.1].

II. Framework and Methodology

The risk analysis audit was performed using a hybrid framework, a combination of OCTAVE Allegro with a Quantitative Analysis method. OCTAVE Allegro with its inherent flexibility allows to customize it to match the organizational standards and requirements and hence it was opted as the risk assessment framework for the risk audit done for Netsys Bank (Pvt.). With its flexibility it allows utilizing both qualitative and quantitative approaches to derive the ideal solutions and controls with the optimal cost-benefit.

To further assist the upper management for their decision-making process, the quantitative risk analysis is included in this report. It will aid them in determine the feasible controls and expected benefit/profit margins after applying these recommended controls and threat mitigation methods.

2. Information Asset Profiles

Asset	Description	Container	Owner(s)	Security Requirement status			
				Property	L	M	H
Firewall	Prevent the transference of inside information and the performance of financial transactions between commercial and investment banks.	**S/W:** Cisco Adaptive Security Appliance Software Version 8.2(3) **H/W:** Cisco ASA5510-K9	Senior Network Engineer	C	✔		
				I		✔	
				A			✔
Storage Services – Cloud Storage	Used to store data analytics and all the data needed for business operations such as currency rates.	**S/W:** ExaVault Cloud FTP **H/W:** Dell EMC ECS	Senior System Administrator	C			✔
				I			✔
				A		✔	
Payment Gateways	This is the cloud-based software that connects the customer to a merchant and is used to capture data, ensure funds are available and pay merchants.	**S/W:** NetPay **H/W:** Dell PowerEdge T40 server	Senior Payment System Operator	C			✔
				I		✔	
				A			✔
Web servers/ FTP server	Hosts client web applications and FTP services which are used by the end-users and management personals to remotely access their data.	**S/W:** Couchdrop servers and Windows Server 2018 **H/W:** Dell PowerEdge T40 server	Senior Network Administrator	C		✔	
				I	✔		
				A			✔
Employee Information Management System	All Employee information which are stored and managed in these databases. Compromising these data can halt all company operations.	**S/W:** SQL Server 2016, Windows Server 2016 **H/W:** Dell PowerEdge T40 server	Human Resource Manager	C			✔
				I			✔
				A			✔

Customer Information Management System	All customer information is stored in this system such as bank account numbers and transaction details. Any compromise to these data can directly affect the business operations.	**S/W:** SQL Server 2016, Windows Server 2016 **H/W:** Dell PowerEdge T40 server	Customer Relations Manager	**C**			✔
				I			✔
				A			✔

3. Analysis of Threat Profiles and Mitigation Strategies

Assets and Asset Value	Threat profile and Vulnerability	Impact Assessment	Identified Controls
Firewall (Cisco ASA5510-K9)	Network Vulnerabilities or configuration errors may lead external attackers into bypass filters and inject malicious data into the system. Cisco ASA VPN module is vulnerable to RCE and reload (reboot).	If compromised the vulnerability might lead to full control over the affected systems.	Regularly update th firewall can keep th firewall safe from attack Update Install the late patched version of AS firmware Cisco Adaptiv Security Applianc Software Version 8.0(5)27
Storage Services– Cloud Storage (ExaVault Cloud FTP)	External attackers using Deridex malware can access the system undetected. Malware attack based on Deridex.	These attackers can access word and excel attachments, which causes macros to download the malware and infect the computers.	Updating FTP credentia regularly can help preve Dridex-based attacks.
Payment Gateways (NetPay)	External attackers maybe able to acquire the emails and passwords of customers and access their user accounts. Prerequisites for online transactions can occur.	User accounts will be tampered with and if the users have saved their credit card details, there can be potential money thefts as well.	Use Card Security Code such as CVV2, CVVC, ar CID. Updating anti-malwa software regularly and us of strong OTPs.
Web Servers/FTP servers (Couchdrop servers and Windows Server 2018)	External attackers may be able to make these services unavailable by attacks like DDoS. Windows Denial of Service Vulnerability	User access portals will be unavailable if a DDoS attack occurs. Users may not be able to access their stored data when they need them.	Install a web applicatio firewall, use WebDAV ar use SFTP instead of FT Update windows server 2019(October 2018).
Employee Information management System (SQL Server 2014, Windows Server 2016)	System failures and malfunctions caused by employee mistakes and poor security practices with the staff exposes the system to both internal and external attacks. System vulnerabilities could be	In this situation, internal management can be corrupt, and employees may lose confidence in the company.	Conduct security be practice workshops for th non-technical sta Redefine the Passwo Policy as follows [Append C, Section C.1]

	exploited by external attackers to alter user information.		
Customer Information Management System (SQL Server 2014, Windows Server 2016)	Internal vulnerabilities could be exploited by external attackers to alter user information. Successful Exploits can allow attackers to execute arbitrary code within the context of the SQL Server Database Engine service account.	Disclosure of private information could lead to violation of the "The General Data Protection Regulation" and there will be legal penalties and fines.	Upgrade SQL Serv version and the Windov Server version running the container. Perfor Monthly security audits ar redefine the Passwo Policy as follows [Append C, Section C.1]

4. Quantitative Analysis

Assets	Asset Value	Before Applying Controls		After Applying Controls	
Firewall (Cisco ASA5510-K9)	$50,000	EF	50%	EF	20%
		SLE	25,000	SLE	10,000
		ARO	0.6	ARO	0.3
		ALE	15,000	ALE	3000
		Cost Benefit = $15,000 – ($3000 + $8000) = $ 4000			
Storage Servers – Cloud (ExaVault Cloud FTP)	$ 2,000,000	EF	12%	EF	8%
		SLE	240,000	SLE	160,000
		ARO	0.42	ARO	0.3
		ALE	100,800	ALE	48,000
		Cost Benefit = $100,800 – ($48,000 + $20,000) = $ 32,800			
Payment Gateways (NetPay)	$ 1,000,000	EF	40%	EF	15%
		SLE	400,000	SLE	150,000
		ARO	0.9	ARO	0.7
		ALE	360,000	ALE	105,000
		Cost Benefit = $360,000 – ($105,000 + $30,000) = $ 225,000			
Web Servers/FTP servers (Couchdrop servers and Windows Server 2018)	$ 200,000	EF	32%	EF	25%
		SLE	64,000	SLE	50,000
		ARO	0.8	ARO	0.6
		ALE	51,200	ALE	30,000
		Cost Benefit = $ 51,200 – ($30,000 + $3000) = $ 18,200			
Employee Information Management System (SQL Server 2014, Windows Server 2016)	$ 50,000	EF	15%	EF	10%
		SLE	10,500	SLE	7000
		ARO	0.5	ARO	0.3
		ALE	5250	ALE	2100
		Cost Benefit = $ 5250 – ($2100 + $2000) = $ 1150			
Customer Information management System (SQL Server 2014, Windows Server 2016)	$ 400,000	EF	30%	EF	10%
		SLE	120,000	SLE	4000
		ARO	0.5	ARO	0.5
		ALE	60,000	ALE	20,000
		Cost Benefit = $ 60,000 – ($20,000 + $15,000) = $ 25,000			

SUMMARY

REFERENCE

APPENDIX

Appendix A

Section A.1

Key Terms and Acronyms

Acronym	Key Term
EF	Exposure Factor
SLE	Single Loss Expectancy
ALE	Annualized Loss Expectancy
ARO	Annualized Rate of Occurrence
SW	Software
HW	Hardware
DDoS	Distributed Denial of Service Attacks
FTP	File Transfer Protocol
SFTP	Secure File Transfer Protocol
CVV2	Card Verification Value 2
CVVC	Card Verification Value Code
CID	Card Identification Number
OTP	One Time Password
C	Confidentiality
I	Integrity
A	Availability
H	High
M	Medium
L	Low

Section A.2 – Qualitative Risk Analysis

The qualitative risk analysis is done prior to identifying assets with the highest Relative Risk Scores. During the process, 6 assets were identified as high-risk level assets as they exceeded the Risk Tolerance Level – Risk Tolerance Level = 4 – to conduct the Threat Profiling and Quantitative Analysis.

The Relative Risk Score was derived as follows.

Relative Risk Score = SUM (Impact Area Score = Impact Area value X Probability)

The sum of all Impact Scores is considered as the Relative Risk Score.

A.2.1 Impact Area Measurement Criteria

Impact Area	Negligible = 1	Low = 2	Medium = 3	High = 4	Critical = 5
Reputation & Customer Confidence	Less than 1% reduction in customers due to loss of confidence.	Less than 5% reduction in customers due to loss of confidence.	5% to 20% reduction in customers due to loss of confidence.	20% to 40% reduction in customers due to loss of confidence.	More than 40% reduction in customers due to loss of confidence.
Finance	Less than 0.5% yearly revenue loss.	Less than 5% yearly revenue loss.	5% to 10% yearly revenue loss.	10% to 30% yearly revenue loss.	More than 30% yearly revenue loss.
Productivity	Staff work hours are increased by less than 1% for maximum one day.	Staff work hours are increased by less than 5% for 7 to 10 day(s).	Staff work hours are increased between 5% and 15% for 10 to 20 days.	Staff work hours are increased between 15% and 30% for 20 to 30 days.	Staff work hours are increased by greater than 30% for more than 30 days.
Health & Safety	The presence of the hazard will not and does not affect any living individual within the organizational infrastructure.	Immediately treatable degradation in customers' or staff members' health with recovery within a day.	Temporary or recoverable impairment of customers' or staff members' health	Permanent impairment of significant aspects of customers' or staff members' health	Results in death of one or more individuals within the organizational infrastructure.

Legal	Less than 0.5% cost of typical yearly revenue.	Less than 3% cost of typical yearly revenue.	3% to 15% cost of typical yearly revenue.	15% to 25% cost of typical yearly revenue.	More than 25% cost of typical yearly revenue.

A.2.2 Probability Measurement Criteria

To determine the Probability factor, a heuristic analysis of all past incident reports and global trends on cyber security threats were performed [].

Very Unlikely	Unlikely	Possible	Almost Certain	Certain
0 – 20%	21% – 40%	41% - 60%	61% - 80%	80% - 100%

A.2.3 Relative Risk Score Calculation

Asset	Probability	Impact Area	Value	Score	Relative Risk Score
Firewall	0.4	Reputation & Customer Confidence	3	1.2	4.8
		Financial	3	1.2	
		Productivity	3	1.2	
		Legal	2	0.8	
		Health & safety	1	0.4	
Storage Servers -Cloud	0.3	Reputation & Customer Confidence	5	1.5	5.1
		Financial	4	1.2	
		Productivity	4	1.2	
		Legal	3	0.9	
		Health & safety	1	0.3	
Payment Gateways	0.25	Reputation & Customer Confidence	5	1.25	4.75
		Financial	5	1.25	
		Productivity	4	1	
		Legal	4	1	
		Health & safety	1	0.25	
Web servers/FTP servers	0.45	Reputation & Customer Confidence	3	1.35	5.85
		Financial	3	1.35	
		Productivity	3	1.35	
		Legal	3	1.35	
		Health & safety	1	0.45	
Employee Information management System	0.3	Reputation & Customer Confidence	3	0.9	4.2
		Financial	3	0.9	
		Productivity	5	1.5	
		Legal	2	0.6	

		Health & safety	1	0.3	
Customer Information management System	0.3	Reputation & Customer Confidence	5	1.5	5.7
		Financial	5	1.5	
		Productivity	4	1.2	
		Legal	4	1.2	
		Health & safety	1	0.3	

Appendix B

Section B.1 – Exposure Factor Calculation Methodology

Here is the guideline used for estimating the Exposure Factor to be used in the Quantitative Risk Analysis Process [].

Start from 100% mark

1. **Does the system under attack have any redundancies/ backups/ copies?**

Subtract 30% if the answer is YES

2. **Is the system under attack behind a firewall?**

Subtract 5% if the answer is YES

3. **Is the attack from outside?**

Subtract 10% if the answer is YES

4. **What is the potential rate of attack? (10% damage / hour)**

Subtract 10% if the answer is less than 20% damage/hr.

Subtract 30% if the answer is less than 2% damage/hr.

5. **What is the likelihood that the attack will go undetected in time for a full recovery?**

Subtract 10% if the probability of being undetected is less than 20%

Subtract 15% if the probability of being undetected is less than 10%

6. **How soon can a countermeasure be implemented in time if at all?**

Subtract 15% if the countermeasure can be implemented within ½ hour

Subtract 10% if the countermeasure can be implemented within 1 hour

Subtract 5% if the countermeasure can be implemented within 2 hours

Section B.2 – Single Loss Expectancy (SLE)

Single Loss Expectancy is the monetary value expected from the occurrence of a risk on an asset [].

SLE = Asset value x Exposure Factor (EF)

Section B.3 – Annualized Rate of Occurrence Calculation

To calculate the Annual Rate of Occurrence Value (ARO) the following list of techniques was used.

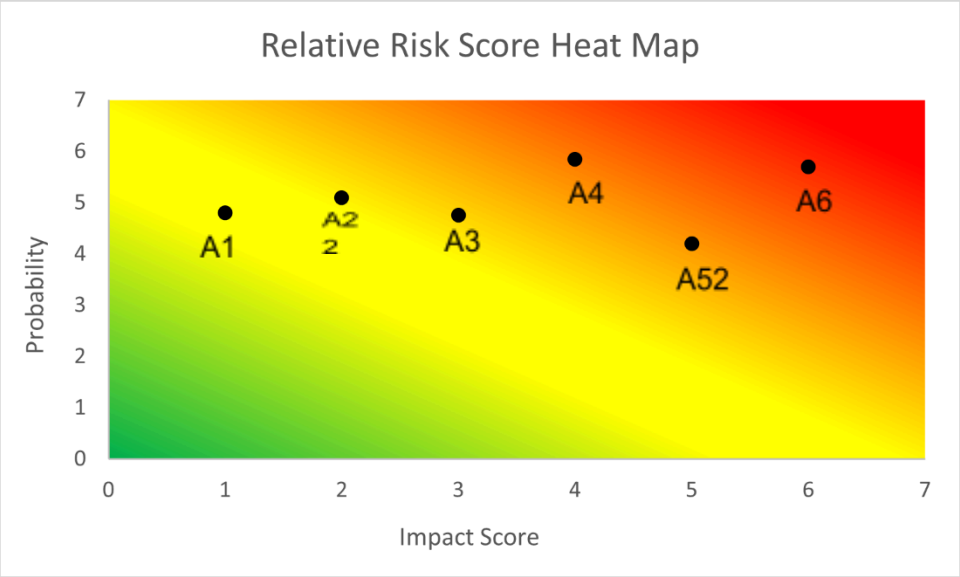
- Analyzing past records of incident reports and firewall log entries
- Conducting questionnaires and conferencing sessions with the security team and technical staff
- Performing penetration tests to examine the existing controls and security features to identify flaws and loopholes

B.3.1 Annualized Loss Expectancy (ALE)

The expected monetary loss for an asset due to a risk over a one-year period.

ALE = Single Loss Expectancy (SLE) X Annual Rate of Occurrence (ARO)

B.4 Relative Risk Score Heat Map



A1 – Firewall
A2 – Storage Servers (cloud)
A3 – Payment Gateways
A4 – Web Servers/ FTP Servers
A5 – Employee Information Management System
A6 – Customer Information Management System

Appendix C – Mitigation Plan

Asset	Containers for apply controls	Controls, Administrative, Technical, and Physical Controls
Firewall	Cisco ASA5510-K9	- Update the firewall software to the latest version of 9.1(7) - Regularly update the firewall ruleset for net threats - Configure Server Security and Firewall Script.
Storage Servers – Cloud	ExaVault Cloud FTP	- Update server software to FreeNAS 11.3 - Update server control panel regularly.
Payment Gateways	NetPay (Bank initiated payment gateway)	- Regularly monitor the data encryption during transactions. - Use Secure Socket layers (SSL) - Use of Secure Electronic Transaction (SET) protocols.
Web servers/FTP servers	Couchdrop servers and Windows Server 2018	- Install a web application firewall, use WebDAV and use SFTP instead of FTP.

		- Update windows server to 2019(October 2018) with the 2020-04 Cumulative Update for Windows Server, version 1903 for x64-based Systems (KB4549951)
Employee Information management System	SQL Server 2014 running on Windows Server 2016.	- Audit and Monitor Database Activity - Update SQL Server to 2019 (KB 4548597) - Update windows server to 2019(October 2018) - Update server control panel regularly - Redefine the existing password policy by adding new set clauses as described in the CIMS mitigation method. - Conduct Informative Workshop Seminar for non-technical staff related to information security best practices.
Customer Information management System	SQL Server 2014 running on Windows Server 2016.	- Update SQL Server to 2019(15.0) with cumulative security patch CU 4 (KB 4548597) - Update windows server to 2019(October 2018) with the 2020-04 Cumulative Update for Windows Server, version 1903 for x64-based Systems (KB4549951) - Update SQL Server to 2019(15.0) - Update windows server to 2019(October 2018) - Auditing in these categories: 1. Audit account logon events. 2. Audit account management. 3. Audit logon events. 4. Audit object access. 5. Audit process tracking - Redefine the existing Password Policy by introducing the following new constraints and features: 1. Password Expiration Policy. 2. Password Complexity Requirement Policy (Demands the use of special characters, numbers, and capital letters in user passwords). SQL Server 2014 running on Windows Server 2016. 3. Password Audit Policy (Enable tracking of password changes by monitoring all user modifications).