RISK ASSESSMENT REPORT (2020)

Executive Summary

During the period March 23 2020 a detailed Information Security Risk Assessment was performed on the Test company LTD

The Mandal Company LTD provide XYZ Services in the exchange of personal identifiable information

The assessment identified several medium risk items the should be addressed by the management

---

DETAILED ASSESSMENT

1.Introduction

1.1 Purpose

The purpose of the risk assessment was to identify threats and vulnerability related to the company Mandal LTD .The risk assessment will be utilised to identify risk mitigation plans treated to Mandal LTD , The PII is identified as a potential risk system in the Department's annual enterprise risk assessment

---

1.2 Scope of the risk assessment

The Mandal Company collect PII on a daily bases from their website that allow the user input data and receive information from the online application web based application developed and maintained by Mandal LTD, This application is build using Microsoft IIS server and uses Active Server Pages . The application has an interface with the and also has payment link. The application component are physically housed in the Mandal LTD Data centre in Australia

The scope of this assessment is includes all the component described above except for the pay link , the pay link interface the compose managed by the Mandal IT department Also in this scope are the supporting system which include DMarkZone(DMZ) network segment and DMZ firewalls. The web application , Mandal LTD database and OS and supporting these components are all in the scope

---

2 Risk Assessment Approach

2.1 Participants

Role	Participant
Sys Admin	Sonu Mandal
Sys Custodian	Suresh Haze
Database Admin	Ravi Dubey
Risk Assessment Team	John Smith , Virat Kohli , Rohit Pandya

2.2 Techniques Used

Technique	Description
Risk Assessment Questionnaire	The Assessment team used a tailored version of the self assessment questionnaire in the in the NIST SP-26 “Security Self Assessment” Guide for information tech system. This questionnaire assisted the team identifying risks.
Assessment Tools	The Assessment Team used several security testing tools to review System configuration and identify Vulnerability in the application the tool included Nmap ,Nessus AppScan
Vulnerability Sources	The Team accessed several vulnerability sources to help identify potential vulnerability . The sources consulted included SANS Top 20 OWASP Top 10 NIST I-CAT Vulnerability Database Microsoft Security Advisories CA Alert Service
Transaction Walkthrough	The Assessment team selected at least one used case of each time and walked each used case through the application process to gain an understanding of the data flow and control points
Interviews	The interviews were conducted to validate information
Review of Documentation	The assessment team reviews Mandal security policies , system documentation network diagrams and operational manuals related the assessment
Site Visit	The Team conducted a site visit at the Data Center and reviews physical access and environmental controls

2.3 Risk Model

In determining risk associated with the Mandal LTD, We utilised the following model for classifying risk

Risk = Likelihood x Severity (Impact)

Sand the following Definitions

Likelihood

Likelihood (weight Factor)	Definition
High (1.0)	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective
Medium (0.5)	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low (0.1)	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

2.4 Risk was calculated as follows

Likelihood	Low (10)	Medium (50)	High (100)
High (1.0)	Low Risk 10 x 1.0 = 10	Medium Risk 50 x 1.0 = 50	High Risk 100 x 1.0 = 100
Medium (0.5)	Low Risk 10 x 0.5 = 5	Medium Risk 50 x 0.5 =25	High Risk 100 x 0.5 = 50
Low (0.1)	Low Risk 10 x 0.1 = 1	Medium Risk 50 x 0.1 = 5	High Risk 100 x 0.1 =10

Risk Scale *High. (> 50 to 100)*
Medium (> 10 to 50)
Low. (> 01 to 10)

2.5 *Simple Risk Matrix*

Likelihood

	Low	Medium	High
High	Medium	High	Critical
Medium	Low	Medium	High
Low	Low	Low	Medium

Impact

Risk level means in business terms.

Impact	Definitions
High	The lose of confidentiality , integrity or availability could be expected to have a severe or catastrophic adverse effect on organisation operations , organisation assists, or individuals Examples : • A severe degradation of loss of mission capability an extent and duration that the organisation is not able to perform one or more of it's primary functions • Major damage to organisational assets • Major financial loss • Severe or catastrophic harm to individual involving loss of life or serious life threatening injuries
Medium	The lose of confidentiality , integrity or availability could be expected to have a severe or catastrophic adverse effect on organisation operations , organisation assists, or individuals Examples : • Significant degradation of loss of mission capability an extent and duration that the organisation is not able to perform one or more of it's primary functions • Significant damage to organisational assets • Significant financial loss • Significant harm to individual involving loss of life or serious life threatening injuries
Low	The lose of confidentiality , integrity or availability could be expected to have a severe or catastrophic adverse effect on organisation operations , organisation assists, or individuals Examples : • A Degradation of loss of mission capability an extent and duration that the organisation is not able to perform one or more of it's primary functions • Minor damage to organisational assets • Minor financial loss • Minor harm to individuals

3. Potential Treat Statement

The team identified the following potential threat-sources and associated threat actions applicable to Mandal LTD PII collection system

Threat-Source	Threat Actions
Hacker	• Web Defacement • Social Engineering • System Intrusion , Break-ins • Unauthorised System access
Insider Threat	• Browsing of personality identifiable information • Malicious code executions • Exploiting Malicious code (e.g., virus) • Exploiting System Bug • Unauthorised System Access
Computer Criminal	• Identify Theft • Spoofing • System Intrusion
Environment	• Natural Disaster • Fire • Flood

3.1 Risk Assessment Results

Item Number	Observation	Threat-source	Existing Controls	Likelihood	Impact	Risk Rating	Recommended controls
1	Cross Site Scripting	Hacker / Password Effectiveness	None	Medium	Medium	Medium	Validation of the all cookie, query springform field, and hidden field (i.e all the parameters) against a rigorous specification if what should be allowed
2	User System Passwords can be guessed or cracked	Hackers	Password should be converted to passphrase format	Medium	Medium	Medium	Required use of special characters
3	Data Could be inappropriately extracted from Mandal LTD Database by entering SQL Command into input field	Hackers /SQL Injection	Limited Validation checks on input	High	Medium	Medium	Ensure that all the parameters are validated before they are used. A centralised component or library is likely to be the most effective, as the code performing the checking should be in one place. Each parameter should be checked against a strict format that specific exactly what input will be allowed
4	Web server and application running unnecessary services	All/ Unnecessary Services	None	Medium	Medium	Medium	Reconfigure System to remove unnecessary services
5	Disaster Recovery plan has not been established	Environmental Disaster Recovery	Weekly Backup Only	Medium	High	Medium	Develop and test a Disaster Recovery Plan