

CYBERSAFE VULNERABILITY ASSESSMENT

Techbrain

Abstract

Organisation undertook self-assessment to understand business's security posture against Essential Eight Maturity Level 1. Based on the input provided, this report outlines existing posture, provides recommendations to achieve the required security posture.

JohnDoe

johndoe@gmail.com

VULNERABILITY ASSESSMENT

Executive Summary

Overview

The Self-assessment tool assessed each of the mitigation strategy based on user input and reported security controls that were not met. An additional section (Project Findings) reports the detailed results of our assessment.

Organisation Techbrain requires implementation of additional security controls to meet the Essential Eight Maturity Level 1 and by not meeting all requirements of the Maturity level 1, organisation Web2web is assessed to be at Essential Eight Maturity Level 0.

It is important to reiterate that this report represents a snapshot of the security posture at the time of testing.

Our team of security specialists, based in Australia, would love to have the opportunity to assist you in implementing the necessary security controls. Should you require assistance please email security@cybersafe.training or call +618 9201 2340

Scoping Restrictions

The engagement primarily focused on self-assessment on:

- Web2web's infrastructure against Essential Eight Maturity Level 1
- The framework used is ACSC's ISM Framework.
- Report is based on input provided by John Doe

Findings Summary


The Self-assessment tool assessed each of the mitigation strategy based on user input and reported security controls that were not met. An additional section (Project Findings) reports the detailed results of our assessment.


VULNERABILITY
ASSESSMENT

Project Findings

As part of the project scope Web2web IT security posture, we conducted the security assessment to collect inventory and client's IT security posture was assessed against ACSC's Essential Eight Maturity Level 2, which is considered the base line for non-corporate Commonwealth entities, the results of the assessment are outlined below.

Key:


 You are likely to meet security control requirements for Maturity Level 1

 You are not likely to meet security control requirements for Maturity Level 1

General questions




Question	Response
What is your infrastructure?	All Cloud, with workstations
Who is responsible for business IT?	MSP
Who is your Cloud Service Provider?	M365
Do you have an IT asset management process and an up to date list of all IT assets owned by the business?	No
Select Operating Systems that are used by the business?	Windows 10 v21H1 & Above
Do you have a vulnerability scanner?	Yes

Application control





Question	Response	Outcome
Can users install applications on their computers?	Yes	

VULNERABILITY ASSESSMENT

Patch applications

Question	Response	Outcome
How often is the vulnerability scanner run?	-	
How often are applications patched?	No schedule, when required	
Do you have any products which are no longer supported by vendors?	No	

Configure Microsoft Office macro settings




Question	Response	Outcome
Do you use Microsoft Office suite?	Yes	
Is Office Macro disabled for users who don't need it?	No	
Is Macro antivirus enabled for all users?	-	
Can users change Office settings?	-	

User application hardening


Question	Response	Outcome
How often is the vulnerability scanner run?	-	
Can users access internet from IE11?	-	
Do users see advertisements when opening any webpages?	-	
Can users change web browser security?	-	

VULNERABILITY ASSESSMENT




Restrict administrative privileges

Question	Response	Outcome
Is Administrator access validated on request?	Yes	
Can Administrators access internet, email & web services?	Yes	
Is there an internal user who has Administrator access?	Yes	

Patch operating systems


Question	Response	Outcome
How are updates applied to devices?	Automatic updates	
When are the updates installed?	Automatically, weekly/monthly	
How often is the vulnerability scanner run?	Manual, ad-hoc	

Multi-factor authentication

Question	Response	Outcome
Do you have any Internet facing services?	Yes	
Do you have MFA on all Internet facing services?	No	
Do all internal & external users require MFA if they access any business Internet facing services such as emails, SharePoint, VPN, RDGateway etc.,?	N/A	

VULNERABILITY ASSESSMENT

Regular backups

Question	Response	Outcome
Do you backup all your important information?	Yes	
Do you test restore your backup periodically?	No	
Who has access to modify/edit the backup?	-	

Recommendations

Short-term Improvements

- System Administration: Implement User access management
- Application Management: Implement Application hardening and Application Control. Create an application update plan.
- Application Hardening: Disable Office Macros for users that do not have a demonstrated business requirement
- Privileged access to systems: administrators are prevented from accessing the internet, email and web services.
- Separate privileged operating environments: create separate privileged and unprivileged accounts for users to use on privileged and unprivileged operating environment.
- Patch Management: Implement a managed and automatic patch management system.
- Vulnerability Management: Implement and Run Internal vulnerability periodic scans and patch/mitigate all identified vulnerability to protect against internal threat.
- Multi-Factor Authentication: Implement MFA (where available) by organisation's users to access any business internet facing services.
- Data Backup & Restoration: create disaster recovery exercises plan and test restoration of systems, software and important data from backup
- CyberSafe awareness training
- Achieve Certified Cybersafe

VULNERABILITY
ASSESSMENT

Long-Term Improvements

- Information Security Awareness Training for employees including
 - Awareness of the organisations policy, including Acceptable Use Policy
 - Conducting Email Phishing Campaign
- Perform a more comprehensive security review of the components not audited during this engagement. This would include working towards Essential Eight Maturity Level 2 & 3 outlined in ACSC's ISM Framework.
- Perform an Information Security Management System (ISMS) Audit (ISO27001:2013)
- Penetration Testing: Internal and external Penetration testing should be undertaken periodically to identify and patch security gaps.

Our team of security specialists, based in Australia, would love to have the opportunity to assist you in implementing the necessary security controls. Should you require assistance please email security@cybersafe.training or call +618 9201 2340

VULNERABILITY ASSESSMENT

Appendix A - Reference links

- Cyber Security Risk Assessments
- Cyber Security Training
- Cyber Security Certification

VULNERABILITY
ASSESSMENT

Thank you,
The Team at Cyber Safe International