Essential Eight Framework – Audit Findings

Hamish Burnett – (222282244)

Contents

Executive Summary

The Essential Eight Framework, is a set of measures that organisations can take, to improve their cyber security posture, and prevent cyber attacks (Australian Signals Directorate and Australian Cyber Security Centre, 2023). This framework was developed by the *Australian Signals Directorate*, which is "an Australian Government intelligence agency, responsible for [...] cyber security", and serves as a baseline, of what an organisation's security posture, should look like (Australian Signals Directorate, n.d.).

The Essential Eight Framework, is broken down into eight categories, being:

- Patching of Applications
- Patching of Operating Systems
- Multi-Factor Authentication
- Restriction of Administrative Privileges
- Application Control
- Restriction of Microsoft Office Macros
- User Application Hardening
- Regular Backups

While the questionnaire was not completed by the deadline, an analysis into the current maturity, of the Chameleon organisation, was performed. It is believed that the Chameleon organisation currently has a maturity rating of zero. Security measures can be implemented, to increase the Essential Eight maturity rating.

While the Chameleon organisation has received a maturity rating of zero, it is believed that the organisation would only be targeted by attackers operating at the level one, maturity rating.

Introduction

The Essential Eight Framework, is a set of measures that organisations can take, to improve their cyber security posture, and prevent cyber attacks (Australian Signals Directorate and Australian Cyber Security Centre, 2023). This framework was developed by the *Australian Signals Directorate*, which is "an Australian Government intelligence agency, responsible for [...] cyber security", and serves as a baseline, of what an organisation's security posture, should look like (Australian Signals Directorate, n.d.).

The Essential Eight Framework, is broken down into eight categories, being:

- Patching of Applications
- Patching of Operating Systems
- Multi-Factor Authentication
- Restriction of Administrative Privileges
- Application Control
- Restriction of Microsoft Office Macros
- User Application Hardening

The Essential Eight Framework, also provides a maturity rating, for the types of attacks that an organisation may be exposed to, and associated controls, along with each level. Higher maturity levels, indicate a higher level of sophistication, within the attacks, which may target organisations.

Essential Eight Framework Analysis

The maturity level of an organisation, is graded between zero, and three, with zero having the lowest levels of security, while level three, containing the highest levels of security.

If an organisation achieves a maturity rating of zero, it indicates that the organisation has vulnerabilities, which may affect the confidentiality, integrity, or availability of, their data, and systems. They are also vulnerable to level one attacks.

If an organisation achieves a maturity rating of one, this indicates that they have some basic security measures in place, to prevent low level attacks. Low level attacks, that align with the level one maturity rating, include attackers that use freely available tools and software, that is accessible to anyone. These attackers will prefer to use tools that are publicly accessible, and will launch automated attacks against a wide variety of organisations, rather than targeting a specific individual organisation.

If an organisation achieves a maturity rating of two, this indicates that the organisation has implemented the level one objectives, and has a basic level of security. Attackers who operate at the second level, of the Essential Eight framework, will be somewhat more persistent, in their attempts to hack a specific organisation, although, they will not dedicate large amounts of time/effort, into attacking a single organisation. These attackers will use common tools, but will also refine the tools that they use, to ensure that they are effective.

If the organisation achieves a maturity rating of three, this indicates that the organisation has implemented the security controls, of the lower levels, and is at a higher risk of more advanced attacks, and high level attackers. The attackers that operate at this level, will spend considerably more effort targeting individual organisations, rather than targeting any organisation, with automated attacks. They will be skillful, and develop their own tools, rather than using common, publicly available tools. These attackers will seek to move around an organisation, remain persistent within an organisation, utilize advanced measures, to gain access, and prevent detection.

At the current stage, it is believed that the Chameleon organisation would generally only be targeted by attackers operating at level one, of the Essential Eight Maturity Model. This is because the Chameleon organisation does not collect, or store any personal data, about users, contains no information that would be valuable to attackers, and is a website that contains very limited functionality. It is believed that the majority of attacks against the Chameleon website, will be low level attacks, using automated tools, and publicly available software.

It is not believed that level two, or level three hackers would attack the website, as there would be nothing worthwhile, to obtain, from attacking the websites of the Chameleon organisation. They would also avoid wasting time, on a low level target.

Methodology

A questionnaire was developed, and distributed to the appropriate individuals, within the Chameleon organisation. The questionnaire that was developed, is shown, under the title: *Essential Eight Questionnaire*.

Essential Eight Questionnaire

The Essential Eight Framework, is a set of measures that organisations can take, to improve their cyber security posture, and prevent cyber attacks (Australian Signals Directorate and Australian Cyber Security Centre, 2023). This framework was developed by the *Australian Signals Directorate*, which is “an Australian Government intelligence agency, responsible for [...] cyber security”, and serves as a baseline, of what an organisation’s security posture, should look like (Australian Signals Directorate, n.d.).

The Essential Eight Framework, is broken down into eight categories, being:

- Patching of Applications
- Patching of Operating Systems
- Multi-Factor Authentication
- Restriction of Administrative Privileges
- Application Control
- Restriction of Microsoft Office Macros
- User Application Hardening
- Regular Backups

This questionnaire, is designed to analyse the current posture, and maturity rating, on the Essential Eight Framework, for the Chameleon organisation. Most of the Essential Eight requirements, have been taken directly from the Essential Eight Maturity Model page (https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model). Some components of the Essential Eight have not been considered, as they are not relevant to the Chameleon organisation.

For the answer to each question, please answer either: **Yes, No, Partially, Unsure, or Not Applicable**. If you wish to provide further information, please feel free to provide further information, in the *More Information* column.

Essential Eight Categories	Questions	Answer	More Information (if necessary)
Patching of Applications	Vulnerability scanning is performed, of the software used to run the applications, and/or GitHub repositories, using an up-to-date vulnerability database.		
	Vulnerability scanning is used, to identify missing patches, or updates, in software that runs the applications, or GitHub repositories.		
	Patches are implemented within 48 hours of being published, when classified as critical.		
	Patches are applied within two weeks, for non critical vulnerabilities.		
Patch Operating Systems	Vulnerability scanning is completed for Cloud environments, and for Operating Systems used within the Cloud, that hosts the website, with an up-to-date vulnerability database.		
	Vulnerability scanning is used to identify missing patches within the Operating Systems, located in the Cloud environments.		
	Critical patches are installed to the Cloud environments, or Operating Systems running inside the Cloud, within 48 hours of being published.		

	Operating systems are retired, once they are no longer supported by the vendor.		
Multi-Factor Authentication	Multi-Factor Authentication is implemented and used, for GitHub, and Cloud environments.		
	The Multi-Factor Authentication consists of something that users know (i.e. a password), and something that they possess (i.e. a text that is sent, which contains a password), or something that a user knows (i.e. password), and are (biometrics, such as fingerprint).		
Administrative Privilege Restrictions	When a user wishes to use elevated privileges, in GitHub, or Cloud environments, they are validated on the first request.		
	Users that require higher privileges are provided a dedicated account, used only for the tasks that require increased privileges, and not for general use.		
	Accounts with elevated privileges, only have elevated privileges to systems that they are allowed to access, and do not provide access to systems that they do not require (i.e. a user may require elevated privileges, to accept Pull Requests, but this user should not be able to use their elevated privileges, to have the power to delete a repository).		
Regular Backups	Data, software applications that have been developed, settings, and operating environments are backed up, to meet business continuity requirements.		
	Backups that have been taken, are stored in a secure manner.		
	Tests are implemented, to ensure that backups can successfully be restored, following an incident.		
	Only privileged accounts, have the functionality to modify and delete backups.		

Outcome of Questionnaire

A response to the questionnaire was not received, by the deadline. Therefore, while the questionnaire remains unanswered, I will make some assumptions, as to the current maturity rating of the Chameleon organisation.

- **Patching of Applications:** I do not believe that the Chameleon organisation would have implemented vulnerability scanning, or implementation of patch, that have been released. This is because the team effectively starts from scratch each trimester (as there is only a single cohort of seniors, who understand the systems, at any one time, and I believe that the development teams would be more focused on achieving deliverables, rather than of the security, of their systems.

- **Patching of Operating Systems:** I believe that this category of would not be met, due ot the reasons above, regarding Patching of Applications.

- **Multi-Factor Authentication:** I believe that the Chameleon organisation may implement multi-factor, as it may be required, by the Cloud provider. It is believed that the Multi-Factor Authentication would consist of a password, and a temporary password, sent by email, or text.

- **Restriction of Administrative Privileges:** Some aspects of the Administrative Privileges Restrictions, may be implemented, while others may not be implemented. It is known that the GitHub pull requests need to be authorized by an authorized member of the team. These authorized members would have elevated privileges, to enable this functionality. The users with elevated permissions, would also sign in to their account, which ensure that the privileges are verified. It is also believed that accounts with higher privileges would be validated, in the Cloud environments. However, it is not believed that the accounts which contain higher privileges, will only be used for the actioning the items which require increased privileges, but will be used, for all normal activities.

- **Regular Backups:** Data may be backed up, as the Cloud environments have the option to configure a wide range of backups, and redundancy measures. However, testing of the backups of the Cloud environment, or GitHub repository, may not be implemented. Thus, in the event of an incident, the effectiveness of restoring from a backup, is not known, in the event of an incident.

From this analysis, it can be seen that security measures may potentially be lacking, within the Chameleon organisation. As a result of these security measures that are not implemented, it is believed that the Chameleon organisation has a maturity level, of zero (0), based on the Essential Eight Framework. While the Chameleon organisation has a rating of zero, it is believed that they would only be facing attacks, in line with level one (1), on the Essential Eight Maturity Model.

Several measures can be taken, to improve the security of the Chameleon organisation, including, patching applications, and Operating Systems, implementing more robust administrative privileges, and performing testing, of backups.

Conclusion

A questionnaire was developed to understand the current maturity level, that the Chameleon organisation achieves, on the Essential Eight Framework. While the questionnaire was not completed by the deadline, an analysis into the current maturity, of the Chameleon organisation, was performed. It is believed that the Chameleon organisation currently has a maturity rating of zero. Security measures can be implemented, to increase the Essential Eight maturity rating.

While the Chameleon organisation has received a maturity rating of zero, it is believed that the organisation would only be targeted by attackers operating at the level one, maturity rating.

References

Australian Signals Directorate (n.d.) *What we do*: Australian Government, accessed 2024. https://www.asd.gov.au/about/what-we-do

Australian Signals Directorate and Australian Cyber Security Centre (2023) *Essential Eight Maturity Model*: Australian Government, accessed 2024. https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model