TECIS60542

Carry out information security vulnerability assessments

Overview

Vulnerabilities provide potential entry points through which a network or application, (typically a web site) can have its functionality or data damaged, downloaded, or manipulated. A typical Web site may have many potential vulnerabilities. Malware (malicious software or code) can be installed by hackers by exploiting security weaknesses to gain access to website and install malicious code.

Vulnerability analysis, also known as vulnerability assessment, is a process that defines, identifies, and classifies the security holes (vulnerabilities) in network or communications infrastructure and in information systems applications. In addition, vulnerability analysis can forecast the effectiveness of proposed information security countermeasures and evaluate their actual effectiveness after they are put into use. Vulnerability assessment seeks to identify both instances of malware on systems as well as system and network-level vulnerabilities.

This standard covers the competencies required to conduct vulnerability assessments and malware scanning. This includes following processes for planning and undertaking vulnerability assessments, prioritising remediation and maintaining up to date vulnerability awareness.

Performance criteria

You must be able to:

1. select and apply the most appropriate methods and tools to be used for malware scanning and vulnerability assessments in line with organisational standards
2. critically review the results of malware scanning and vulnerability assessments, identifying priorities for remediation activity
3. assess vulnerability intelligence information in order to determine the potential impact to the organisation's information systems and network infrastructure
4. communicate vulnerability assessment outputs informing appropriate stakeholders of the potential impact to networks and information systems
5. make recommendations for remediation activities in response to identified vulnerabilities in line with organisational standards
6. recommend improvements to the organisation's information systems and network infrastructure to reduce the future risks associated with identified vulnerabilities
7. ensure that agreed improvements to the organisation's information systems infrastructure and assets are implemented in a timely manner
8. apply the outputs of vulnerability assessments to inform the planning and scheduling of information security testing, operational security and information security management programmes

Knowledge and understanding

You need to know and understand:

1. the range of information assets on which vulnerability assessments need to be conducted
2. the range of vulnerabilities that may compromise an organisation's infrastructure and information assets
3. the range of scanning activities that can be used to identify vulnerabilities and malware in an organisation's information systems and networks and how to apply them
4. how to monitor and assess information in external vulnerability reports to identify relevant vulnerabilities that may need to be investigated and rectified
5. how to distribute warning material to relevant operations functions relating to information security vulnerabilities in a timely manner and suitable for the target audience
6. how to present and communicate vulnerability detection and mediation activities to sponsors and stakeholders
7. how to identify the potential business impacts if vulnerabilities are exploited
8. the fact that new threats and vulnerabilities may emerge at any time
9. the importance of prioritising critical vulnerabilities and recommending timely action to mitigate these
10. the role of vulnerability assessment activities in informing and directing countermeasures to maintain and reinforce information security resilience
11. the importance of ensuring that processes and procedures are implemented and followed to restrict the knowledge of new vulnerabilities externally until appropriate remediation or mitigation is available

Carry out information security vulnerability assessments

Developed by	e-skills
Version Number	1
Date Approved	March 2016
Indicative Review Date	April 2019
Validity	Current
Status	Original
Originating Organisation	The Tech Partnership
Original URN	TECIS60542
Relevant Occupations	Information and Communication Technology; Information and Communication Technology Officer; Information and Communication Technology Professionals
Suite	Information Security
Keywords	Information security, cyber security, vulnerability assessment