Zertifikatsprogramm der Österreichischen Computer Gesellschaft

OCG IT-Security

Syllabus Version 1.0

OCG
Österreichische Computer Gesellschaft
Wollzeile 1-3
A 1010 Wien
Tel: +43 (0)1 512 02 35-50
Fax: +43 (0)1 512 02 35-59
E-Mail: ocg@ocg.at

Web: www.ocg.at

Haftung
Die OCG hat dieses Dokument mit Sorgfalt erstellt, kann aber weder Richtigkeit und Vollständigkeit der enthaltenen Informationen zusichern noch Haftung für durch diese Informationen verursachte Schäden übernehmen. In Zweifelsfällen gilt die Version der OCG, veröffentlicht auf www.ocg.at

Urheberrecht
© Österreichische Computer Gesellschaft (OCG) 2008
Alle Rechte vorbehalten.
Dieser Syllabus darf nur in Zusammenhang mit dem Zertifikatsprogramm der OCG verwendet werden.

Geschlechtsbezogene Aussagen in diesem Syllabus sind auf Grund der Gleichstellung für beiderlei Geschlechter aufzufassen bzw. auszulegen.

Der Syllabus wurde in Zusammenarbeit mit dem ersten Kompetenzzentrum für organisatorische und technische Aspekte von IT-Security, Secure Business Austria (SBA), sowie in Abstimmung mit dem Zentrum für sichere Informationstechnologie, A-SIT, erstellt.

OCG IT-Security

Syllabus 1.0

Ziele

Zielgruppe für das OCG Zertifikat IT-Security sind Computeranwender, die sich mit den wichtigsten Sicherheitsaspekten im Umgang mit Informations- und Kommunikationstechnologien vertraut machen wollen.

Ziel des Zertifikats ist es, das Vertrauen der Benutzer in IT und Internetanwendungen zu erhöhen und gleichzeitig das Wissen um die Gefahren und deren Vermeidung bei der täglichen Arbeit zu verbessern.

Voraussetzungen sind ein allgemeines Grundwissen über Personal Computer und Betriebssysteme, Basiswissen über gängige Office-Anwendungen sowie über die Nutzung von Internet und E-Mail-Diensten.

Die Inhalte von OCG IT-Security sind speziell an den Endbenutzer angepasst und ermöglichen eine praxisrelevante Steigerung des Wissens um die wichtigsten Aspekte der IT-Sicherheit im Umgang mit vernetzten Computersystemen. Dabei werden technische Hintergründe nur soweit behandelt, wie sie für das Grundverständnis der Probleme und Lösungsmöglichkeiten unerlässlich sind.

Kategorie	Fertigkeit	Ref.	Fähigkeit
1 Informations sicherheit	1.1 Wert von Informationen	1.1.1	Den Wert von Daten und Informationen abschätzen können
		1.1.2	Informationen klassifizieren
		1.1.3	Grundsätzlichen Umgang mit Risiken verstehen
	1.2 Anforderungen an die Informations-sicherheit	1.2.1	Vertraulichkeit, Integrität und Verfügbarkeit verstehen
		1.2.2	Die Anforderung nach Nicht-Abstreitbarkeit, Nachvollziehbarkeit, Authentizität verstehen
2 Verschiedene Bedrohungen kennen	2.1 Umwelt	2.1.1	Bedrohung von Daten durch höhere Gewalt kennen
		2.1.2	Bedrohungen der Infrastruktur kennen
	2.2 Personen	2.2.1	Bedrohung von Daten durch interne Personen verstehen
		2.2.2	Bedrohung von Daten durch Mittler verstehen wie zB Wartungspersonal, Zeitarbeiter, Praktikanten
		2.2.3	Bedrohung von Daten durch externe Personen verstehen

Kategorie	Fertigkeit	Ref.	Fähigkeit
3 Wichtige Begriffe kennen	3.1 Grundsätzliches Verständnis	3.1.1	Wichtige allgemeine Begriffe der IT-Sicherheit kennen und verstehen
		3.1.2	Phishing, Malicious Code: Begriffe aus der Welt der Hacker und Script-Kiddies kennen und verstehen
		3.1.3	Wichtige Begriffe der Kryptographie verstehen
4 Social Engineering	4.1 Social Engineering	4.1.1	Social Engineering Angriffe verstehen und vermeiden
		4.1.2	Dumpster Diving und Shoulder Surfing erkennen und vermeiden
5 IT-Sicherheit in der Praxis anwenden	5.1 Sicherheit im Betriebssystem	5.1.1	Merkmale eines guten Passworts kennen
		5.1.2	Das Ereignisprotokoll überprüfen können
		5.1.3	Dateien und Ordnern vollständig löschen können
		5.1.4	Bedeutung unterschiedlicher Benutzerrechte verstehen
	5.2 Eine Personal Firewall verstehen und verwenden	5.2.1	Möglichkeiten und Einschränkungen von Personal Firewalls kennen
		5.2.2	Aufbau und Verwendung von IP-Adressen und Ports verstehen
		5.2.3	Meldungen und Nachfragen von Personal Firewalls verstehen
		5.2.4	Eine Personal Firewall installieren und konfigurieren
	5.3 Einen Virenscanner auswählen	5.3.1	Grundsätzliche Funktionsweise von Virenscannern verstehen
		5.3.2	Kriterien für die Auswahl von Virenscannern kennen
		5.3.3	Grenzen der Virenscanner kennen
	5.4 Sicherheit in Anwendungen	5.4.1	Die Gefahren von aktiven Inhalten verstehen und vermeiden

Kategorie	Fertigkeit	Ref.	Fähigkeit
		5.4.2	Passwortschutz in Office-Produkten einsetzen und verstehen
		5.4.3	Unerwünschte Spuren in Office- und Adobe Acrobat-Dokumenten vermeiden
		5.4.4	Dokumenten-Signatur verstehen und anwenden
	5.5 E-Mail-Sicherheit	5.5.1	Unterschied zwischen Signieren und Verschlüsseln verstehen
		5.5.2	Eine E-Mail ver- bzw. entschlüsseln
		5.5.3	Eine E-Mail signieren
		5.5.4	E-Mail-Sicherheit konfigurieren
		5.5.5	Phishing-Angriffe erkennen
	5.6 Web-Sicherheit	5.6.1	Internet-Zonen einrichten
		5.6.2	Cross Site Scripting-Angriffe erkennen
		5.6.3	Zertifikate von Webseiten prüfen
		5.6.4	Kreditkarten im Internet sicher benutzen
		5.6.5	Die Gefahren von Online-Versteigerungen und Online-Shopping richtig einschätzen und vermeiden
		5.6.6	Eine URL (Unified Ressource Locator) lesen und interpretieren können
6 Mobile Sicherheit	6.1 Laptop	6.1.1	Daten auf Laptops verschlüsseln und absichern
	6.2 PDA und Smartphone	6.2.1	PDA-Daten absichern und verschlüsseln
	6.3 WLAN und WIFI Sicherheit	6.3.1	Unsichere WLANs (Wireless LAN) verstehen und erkennen
		6.3.2	Schwächen von WEP (Wireless Encryption Protocol), Mac (Media Access Control)-Filter und WPA (Wi-Fi protected access) verstehen
		6.3.3	Sicheres WLAN mit WPA konfigurieren
	6.4 VPNs	6.4.1	VPNs (Virtuelle Private Netzwerke) verstehen
		6.4.2	VPN-Verbindungen überprüfen
	6.5 Firewalls	6.5.1	Funktion einer Firmen-Firewall verstehen

Kategorie	Fertigkeit	Ref.	Fähigkeit
		6.5.2	Ein Heimnetz sicher mit dem Internet verbinden
7 Physische Sicherheit und Datensicherheit	7.1 Physische Schutzmaßnahmen	7.1.1	PC-Komponenten physisch sichern
		7.1.2	Physische Sicherheitsmaßnahmen bei mobilen Geräten verwenden
		7.1.3	Physische Schutzmaßnahmen in Gebäuden erkennen und überprüfen
	7.2 Datensicherheit	7.2.1	Möglichkeiten der Datensicherung kennen und unterscheiden können
		7.2.2	Eine Datensicherungsstrategie verstehen und planen können
		7.2.3	Richtiges Verhalten im Falle eines Datenverlustes
		7.2.4	Backup wichtiger Daten und Systeminformationen anlegen
		7.2.5	Durchführung der Backup-Jobs kontrollieren und Backup auf Korrektheit prüfen
		7.2.6	Magnetische Medien (Datenträger) richtig entsorgen
		7.2.7	Optische Medien sicher entsorgen