OCG-IT-Security-Zertifikat für Nutzer

Philippe Benditsch / Gerald Futschek / Markus Klemen / Edgar Weippl

Secure Business Austria, Österreichische Computer Gesellschaft (OCG), Technische Universität Wien
weippl@securityresearch.at, futschek@ifs.tuwien.ac.at

Schlagworte: IT Sicherheit, Security Zertifikat, E-Learning
Abstract: Ziel des IT-Security-Zertifikats ist sowohl die Erweiterung der IT-Kompetenzen von Anwendern als auch die Einführung eines messbaren und international anerkannten Standards.

1. Motivation für das Zertifikat

In den Medien wird immer wieder von Systemausfällen in der IT, groß angelegtem Betrug über E-Mail oder SMS sowie von unbeabsichtigten Veröffentlichungen oder Verlust sensibler Informationen und Daten berichtet. In der Regel sind an gelungenen Attacken auf IT-Systeme die Computeranwender beteiligt, da sie aus Unwissenheit und aufgrund mangelnder Fertigkeiten Situationen nicht richtig einschätzen und entsprechend reagieren können. Von der OCG wurde daher ein IT-Security-Zertifikat für Nutzer entwickelt, die in den bisherigen Zertifizierungen für IT-Profis nicht berücksichtigt worden waren. Für gewöhnlich befasst sich ein Anwender wenig bis gar nicht mit dem Thema IT-Security und ist somit sehr anfällig für Angriffe.

2. Ziel des Zertifikats

Das Ziel des Zertifikats ist sowohl die Erweiterung der IT-Kompetenzen von Anwendern als auch die Einführung eines messbaren und international anerkannten Standards. Dabei wird ein Niveau angestrebt, das vor allem Sicherheitsbewusstsein sowie einen Überblick über die Thematik schaffen soll. Folglich wird auf vertiefende technische Details verzichtet und vorrangig praxisorientiertes Anwenderwissen vermittelt. Experten aus Wissenschaft und Wirtschaft sowie die Kooperation zwischen Secure Business

Austria (ein TU-nahes Forschungszentrum), der OCG und dem A-SIT gewährleisten hohe Qualität.

Wichtiges Ziel des Skriptums ist es, Bewusstsein und Interesse für sicherheitsrelevante Themen zu wecken. Gerade im IT-Bereich gibt es laufend neue Bedrohungen, deren Bekämpfung eine aktive Anteilnahme an den Entwicklungen auf dem Bereich der IT-Security erfordert.

3. Vorteile für Anwender und Unternehmen

Das Erweitern des eigenen IT-Anwenderwissens als auch die international anerkannte Qualifikation in Form einer solchen Zertifizierung sind hinsichtlich aktueller und zukünftiger Berufsaussichten von großem Vorteil. Insbesondere für Berufsgruppen, die mit sensiblen Informationen arbeiten – etwa Rechtsanwälte, Ärzte, öffentliche Stellen oder Mitarbeiter aus dem Finanz- oder Dienstleistungssektor – ist eine solche Zertifizierung ein wichtiger Beitrag zur allgemeinen Sicherheit.

Für Unternehmen stellt das Zertifikat eine messbare Qualifikation potenzieller Mitarbeiter dar. Weiters werden Verständnis und Bewusstsein für die im Unternehmen angewandten Sicherheitsmaßnahmen gefördert. Da diese Sicherheitsmaßnahmen heutzutage bei Weitem nicht mehr ausreichen, müssen Mitarbeiter gegen Social Engineering und auf sensiblen Umgang mit Daten und Informationen geschult werden.

Das Zertifikat sichert einen aktuellen Überblick über sicherheitsrelevante Themen und Techniken sowie grundlegende Anwenderfertigkeiten in der IT-Security. Zielgruppe sind Mitarbeiter von Firmen oder auch Heimanwender, die verstärkt IT-Systeme einsetzen und somit von mehr Sicherheitsbewußtsein profitieren können.

4. Inhalt des Zertifikats

Das Zertifikat deckt folgende Abschnitte ab:

1. Informationssicherheit: Definition der Begriffe Daten und Informationen sowie deren Klassifizierung; Erläuterung von wertbestimmenden Faktoren wie Personalkosten oder Geschäftsprozessen; Erklärung und Abgrenzung von Begriffen wie Vertraulichkeit, Integrität und Verfügbarkeit

2. Bedrohungen von Daten: Benennung von inneren und äußeren Gefahren, Erhöhung des Sicherheitsbewusstseins
3. Wichtige Begriffe: Definition gebräuchlicher Begriffe wie Spoofing, Session Hijacking, digitale Signatur, Policies, Spam, Würmer; Beispiele für Phishing E-Mails
4. Social Engineering: Erklärung sozialer Komponenten wie Dumpster Diving oder Shoulder Surfing; Verhaltensmuster der Angriffe und grundlegende Gegenmaßnahmen
5. Praktische Anwendung von IT-Sicherheit: Wahl starker Passwörter und deren sichere Verwaltung; sicheres Löschen von Daten; Umgang mit Virenscannern, Personal Firewalls, Verschlüsselung und Schutzmechanismen von Microsoft Office und Adobe Acrobat; Verschlüsselung von Nachrichten und Dokumenten und deren Übertragung; sicheres Einkaufen im Internet
6. Mobile Sicherheit: Verschlüsselung von Daten auf Laptops und anderen mobilen Geräten wie Personal Digital Assistants (PDA); Sicherheitseinstellungen von WLAN; Virtuelle Private Netzwerke; Funktion von Firmen Firewalls
7. Physische Sicherheit und Backups: physischen Schutzmaßnahmen bei mobilen und Standgeräten; Datensicherungsmedien und -strategien.

Das OCG-IT-Security-Zertifikats[1] wird mittels Schulung in einer von der OCG autorisierten Institution sowie der positiven Absolvierung einer standardisierten Prüfung erworben.

Die Autoren hoffen, mit der Entwicklung dieses Zertifikats einen Beitrag zur Steigerung der IT-Security bei Computeranwendern geleistet zu haben.

1 Das OCG-IT-Security-Zertifikat http://www.ocg.at/zertifikate/.