SC405 Hacking Professional für Manager & Auditoren

Kurzbeschreibung:

Lernen Sie in diesem Seminar wie ein Hacker zu denken, verstehen Sie deren Absichten und Vorgehensweisen. Erfahren Sie durch eigenes Anwenden, mit welchen Techniken Hacker arbeiten. Nutzen Sie diese Kenntnisse bei Ihren Audits und bauen Sie optimale Schutzmaßnahmen auf. Gleichzeitig lernen Sie, Ihre Ermittlungen effizienter zu gestalten.

Zielgruppe:

Das Basisseminar richtet sich an Datenschützer, ISMS-Beauftragte und -Auditoren sowie alle anderen, die sich bisher eher auf konzeptioneller Ebene dem Thema der Daten- und IT-Sicherheit genähert haben. Nun möchten Sie Vorgehensweisen, Methoden und Techniken von Hackern kennenlernen und verstehen, um die Gefährdung betreuter Systeme sowie die Wirksamkeit von Abwehrmaßnahmen besser einschätzen zu können. Sinnvoll ist das vermittelte Wissen auch für Administratoren, Programmierer und andere IT-Spezialisten, die Einfluss auf die Gestaltung von Programmen, Systemen und Netzwerken haben und Sicherheitslücken verstehen wollen, um sie zu vermeiden.

Voraussetzungen:

Die Teilnehmer sollten grundlegende Kenntnisse über den Aufbau von Computersystemen und Netzwerken haben.

Sonstiges:

Dauer: 3 Tage

Preis: 1690 Euro plus Mwst.

Ziele:

Sie erhalten einen Blick auf Computernetzwerke und IT-Systeme aus Sicht eines Angreifers.

Sie kennen nach dem Seminar Motive, grundlegende Methoden, Vorgehensweisen und Techniken von Hackern und können diese in ausgewählten Beispielen in einer Übungsumgebung selbst praktisch anwenden.

Inhalte/Agenda:

- ♦ Im Verlauf dieses Seminars erfahren Sie, was unter dem Begriff Hacking zu verstehen ist, welche unterschiedlichen Ziele Hacker verfolgen und welche Vorgehensweisen sich daraus ergeben. Sie erlernen den stufenweisen Prozess von der ersten Informationsgewinnung bis zum Aufrechterhalten des erlangten Zugriffes.

- ♦ Nach dieser Einführung werden die notwendigen Grundlagen des Aufbaus von Netzwerken und Serverdiensten vermittelt. Anschließend werden verschiedene Methoden und Techniken wie Footprinting, Fingerprinting, Schwachstellenanalyse, Man-In-The-Middle-Angriffe, Knacken von Passwörtern usw. behandelt. Dabei erarbeiten Sie unter Anleitung des Trainers in der Gruppe gemeinsam den Lösungsweg und können die Attacken selbst mittels verschiedener Tools über das Netzwerk und auf lokale Anwendungen durchführen.

- ♦ Ein besonderes Teilgebiet ist der Datendiebstahl und die Gefahr, die diesbezüglich vor allem von Innentätern ausgeht. Sie lernen Möglichkeiten kennen, wie Daten unbemerkt aus geschützten IT-Systemen herausgebracht werden können.

- ♦