Vorlesungsbeschreibung Wahlpflicht: Social Engineering

Lernergebnisse

Lernergebnisse: Nach dem Modul können die Studierenden verschiedene Ansätze von Social Engineering analysieren und verstehen. Den Studierenden werden Möglichkeiten und Grenzen der sozialen Manipulation in digitalen Umgebungen aufgezeigt. Die Lernenden erwerben die Fähigkeit, Social Engineering in ganz unterschiedlichen Fallbeispielen selbständig zu erkennen und Abwehrmethoden zu entwickeln. Dabei geht es sowohl um allgemeingesellschaftliche Gestaltung, als auch um anwendungsorientierte Fälle. Sie beherrschen die theoretischen Grundlagen, um diese kognitiv, intuitiv und kreativ in der Studienarbeit umzusetzen.

Inhalte

Den Studierenden werden zu folgenden Themen Informationen vermittelt:
Social Engineering sowohl als Gesellschaftsgestaltung , als auch im kleinen Fall , d.h. in Form eines Angriffs auf digitale Firmeninfrastruktur via Menschen (d.h. Mitarbeiter, Externe, Partner, etc.)

Lehrmethoden

Vorlesung, Übungen in Kleingruppen.

Lehrsprache

Deutsch

Studien-/Prüfungsleistung

Hausarbeit oder mündliche Prüfung.

Credits

3
(90 h = 30 h Präsenz- und 60 h Eigenstudium)

Literatur

Baumann, U., Schimmer, K., Fendl, A. (Hg.): SAP Pocketseminar: Faktor Mensch. Die Kunst

des Hackens oder warum Firewalls nichts nützen. SAP 2005 (PDF)

Conheady, S.: Social Engineering in IT Security: Tools, Tactics and Techniques. McGraw-Hill Education, 2014

Duff, A.: Social Engineering in the Information Age. The Information Society, 21: 67-71, 2005

Ekman, P. & Hadnagy, C.: Social Engineering enttarnt: Sicherheitsrisiko Mensch. mitp Professional, 2014

Lardschneider, M.: Social Engineering. Datenschutz und Datensicherheit DuD. 09/2008, 32/9, S. 574-578

Schumacher, S.: Psychologische Grundlagen des Social Engineering. Datenschleuder 94/2010, S. 52-59. Siehe dazu auch: Schumacher, S.: Die psychologischen Grundlagen des Social Engineerings. Magdeburger Journal zur Sicherheitsforschung, Bd. 1, 2011, S. 1 26

Alle öffnen Alle schließen