

IT-Sicherheit im Wintersemester 2018/2019

Übungsblatt 5

Abgabetermin: 27.11.2018 um 12:00 Uhr

Aufgabe 11: (K) Social Engineering

In der Vorlesung wurde ausführlich das Thema *Social Engineering* vorgestellt.

- Nennen und erläutern Sie Kriterien bzw. leiten Sie daraus Kategorien ab, in die sich Social Engineering Angriffe sinnvoll einteilen lassen.
- Eine Möglichkeit, dass ein Social Engineer an sensible Informationen gelangt, ist *Phishing*. Erläutern Sie die Phishing-Varianten *Clone phishing*, *Spear phishing* und *Whaling*.
- Nennen Sie mindestens 4 Dinge, die eine Phishing-E-Mail aufweisen sollte, damit der Social Engineer sein Ziel, d.h. das Erlangen sensibler Informationen, z.B. Zugangsdaten, erreicht.
- Als wirkungsvollste Maßnahme gegen Social Engineering Angriffen gilt nach wie vor, Mitarbeiter zu sensibilisieren und der Aufbau eines Security Awareness Programms. In der vom SANS-Institut herausgegebenen *Top 20 Security Controls* Liste wird auch das Control *Security Skills Assessment and Appropriate Training to Fill Gaps* angeführt. Nennen und erläutern Sie die insgesamt fünf wichtigen Aspekte, diese Maßnahme erfolgreich umzusetzen.

Aufgabe 12: (K) Rechtliche Randbedingungen der IT-Sicherheit

In der Vorlesung haben Sie sich auch mit einigen rechtlichen Rahmenbedingungen auseinander gesetzt. Beantworten Sie dazu folgende Fragen:

- Beschreiben Sie die Unterschiede zwischen Nutzungsdaten (§15TMG), Bestandsdaten (§14TMG) und Inhaltsdaten (BDSG, LDSGe).
- Sie arbeiten in einem Consulting-Unternehmen, das Kunden auch in IT-Sicherheitsthemen berät. Um Ihren Kunden die Brisanz dieses Themas zu verdeutlichen, sind Sie im Besitz eines sogenannten Sniffer-Werkzeugs, um damit Datenpakete aus einem WLAN-Netz zu empfangen, d.h. auch Daten, die eigentlich für andere Empfänger bestimmt sind. Mithilfe dieser Datenpakete und einem weiteren, speziellen Tool kann der Zugangscod des WLAN entschlüsselt werden. Wie beurteilen Sie diese Situation strafrechtlich im Hinblick auf die Paragraphen §202b StGB und §202c StGB?
- Das in Teilaufgabe b) beschriebene Werkzeug ist auf einer ausländischen Internetseite als Open Source Programm frei zugänglich und kann von dort heruntergeladen werden. Sie geben dem Sicherheitsbeauftragten eines Kunden den Link zu dieser Internetseite. Wie beurteilen Sie diesen Tatbestand nach §202c StGB?