Ludwig-Maximilians-Universität München
Institut für Informatik
Lehr- und Forschungseinheit für Kommunikationssysteme und Systemprogrammierung
Prof. Dr. Helmut Reiser

MNM TEAM
Munich Network Management Team

IT-Sicherheit im Wintersemester 2021/2022
Übungsblatt 6

Besprechung: Di, 07.12.2021 um 12:00 Uhr

Aufgabe 23: (T) Social Engineering

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

a. Ein vom Social Engineer häufig angewandtes und in der Praxis erfolgreiche Vorgehensweise ist das *Phishing*. Erläutern Sie die Vorgehensweise und die Unterschiede der Phishing-Varianten *Clone phishing*, *Spear phishing* und *Whaling*.

b. 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.

c. Als wirkungsvollste Maßnahme gegen Social Engineering Angriffen gilt nach wie vor, Mitarbeiter:innen zu sensiblisieren. Der Aufbau eines erfolgreichen Security Awareness Programms ist aber eine Herausforderung. In der vom SANS-Institut herausgegebenen *Top 20 Security Controls* Liste wird auch das Control *Implement a Security Awareness and Training Program* angeführt. Wie sollten Sie demnach beim Aufbau eines Awareness-Programms vorgehen?

Aufgabe 24: (T) Rechtliche Randbedingungen der IT-Sicherheit

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

a. Der Branchenverband BITKOM hat einen praktischen Leitfaden für die Bewertung von Software im Hinblick auf den §202c StGB (Hackerparagraph) veröffentlicht. Obwohl der Verband die Regelung grundsätzlich begrüßt, sieht er dennoch eine Problematik bei deren strikter (im Wortlaut) Anwendung?

b. Erläutern Sie das im BITKOM-Leitfaden definierte, dreistufige Bewertungsschema, inwieweit der Umgang mit einer Software als tatsächlich strafbar zu bewerten ist.

c. Wenden Sie das Bewertungsschema auf einen *Passwort Cracker*, *Schwachstellenscanner* und ein in der Softwareentwicklung häufig eingesetztes *Code Analyse Werkzeug* exemplarisch an.

Aufgabe 25: (T) Datenschutz

Durch die Datenschutz-Grundverordnung (DSGVO), die im Mai 2018 wirksam wurde, gab es in einigen Unternehmen größere Veränderungen im Umgang mit personenbezogenen Daten zu beobachten.

a. Welche Grundsätze für die Verarbeitung personenbezogener Daten schreibt die DSGVO vor?

b. Was ist eine Verarbeitungstätigkeit und zu was sind Organisationen diesbezüglich verpflichtet?

c. Was ist eine Datenschutzfolgenabschätzung und wann ist sie erforderlich?

d. Passiert eine Datenpanne - was ist dann zu tun? Lassen sich existierende Prozesse in der Organisation hier nutzen?

Aufgabe 26: (T) Pentesting

Die Durchführung von Penetrationstests oder kurz *Pen-Tests* ist ein verbreiteter Ansatz von IT-Sicherheitsexperten.

a. Welche Ziele haben Penetrationstests? Welche Risiken bergen sie?

b. Welche Eigenschaften und Qualifikationen sollte ein Pen-Tester mitbringen?

c. Was kann man aus Pen-Test-Ergebnissen lernen? Ist deren Durchführung sinnvoll?

d. Wie unterscheiden sich Pen-Test und Vulnerability Scan?

e. Was sind Blackbox- bzw. Whitebox-Tests? Wann sollte welches Modell angewandt werden?

Aufgabe 27: (H) Selbsttest: Social Engineering

Beim *Social Engineering* richten sich die Angriffe nicht direkt gegen technische Systeme, sondern auf ihre Benutzer.

a. Beschreiben Sie fünf gängige Angriffstechniken des Social Engineerings.

b. Welche davon erscheinen für welche Zielsetzung am erfolgsversprechenden?

c. Selbsttest: Versuchen Sie sich selbst in verschiedenen Social Engineering-Techniken.
Zum Einstieg:

   (i) Shoulder surfing: Was macht der Sitznachbar an seinem Handy in der U-Bahn? Welche Informationen können Sie über den Kommilitonen vor Ihnen anhand seines Laptops innerhalb von fünf Minuten erlangen?

   (ii) Tailgating: Ïch habe meinen Schlüssel vergessen"klappt nie?

   Führen Sie dieses Übungsblatt während Ihrer Versuche vorsichthalber mit sich. ;-)
   (Sollte ein derartiges Blatt als Legitimation ausreichen?)

d. Welche Maßnahmen lassen sich (aus Unternehmenssicht) gegen die verschiedenen Techniken etablieren? Wie kann man sich (als potentielles Opfer) im Alltag schützen?