Reaktive Sicherheit

Übungsblatt 1

Balduin Binder [s6babind@uni-bonn.de] Charlotte Mädler [s6chmaed@uni-bonn.de]
Bünyamin Sarikaya [s6busari@uni-bonn.de]

Aufgabe 1

Aufgabe 1.1

Claudia Eckert benutzt bei ihrer Defintion den Begriff eines *Funktionssicheren* Systems, der jedoch nicht weiter erläutert wird. Das BSI hingegen definiert die Sicherheit eines Systems so, dass die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit, welche die wesentlichen Schutzziele der IT-Sicherheit sind, gewahrt werden. In der Definition von Klaudia Eckert wird nicht konkret auf Schutzziele eingegangen. Man könnte die Definition von Klaudia Eckert als abgeschwächte Beschreibungen der beiden Schutzziele Integrität und Vertraulichkeit ansehen, jedoch ist diese in ihrer Formulierung zu ungenau. Das BSI definiert die IT-Sicherheit außerdem weitreichender und spricht von *Informationssicherheit*. Hierbei geht es primär um die Sicherheit einer Information und den Schutz (bezüglich der zuvor genannten Schutzziele) einer Information und nicht nur die eines Systems.

Aufgabe 1.2

- **Vertraulichkeit:** Signal Nachrichten sind end-zu-end Verschlüsselt, heißt nur Empfänger und Sender haben den Schlüssel der Notwendig ist die Nachricht zu lesen, dritten ist es so nicht ohne weiteres möglich den Inhalt zu lesen.
- **Integrität:** Alice signiert ihre Emails an Bob mit ihrem geheimen Schlüssel, somit kann Bob sich sicher sein, dass die Email wirklich von Alice stammt. Das Schutzziel Integrität ist gewährleistet, da niemand die Information aus der E-Mail verändern kann ohne den geheimen Schlüssel von Alice zu besitzen.
- **Verfügbarkeit:** Alice macht immer Backups von ihren Daten, somit kann sie sich sicher sein, dass ihre Daten verfügbar sind, falls ihr Computer mal crashen sollte.
- **Authentizität:** Alice signiert ihre Email an Bob mit ihrem geheimen Schlüssel, somit kann Bob überprüfen ob Alice die Email geschrieben hat. Die Email stammt also nachweislich von Alice, somit ist das Schutzziel der Authentizität gewährleistet.
- **Zurechenbarkeit:** In einem Online-Forum X müssen sich alle Teilnehmer mit ihrem Ausweis registrieren und dürfen keine Nick-Names benutzen. Jeder kann nun jeden Post in diesem Forum eindeutig einer Person zuordnen, somit ist das Schutzziel der Zurechenbarkeit gewährleistet.

Aufgabe 2

- **Digitaler Identitätsdiebstahl:** Die missbräuchliche Nutzung personenbezogener Daten durch Dritte im digitalen Raum (Internet). Im realen Leben kann dies so aussehen, dass Dritte Passwörter stehlen und sich mit diesen auf Internetseiten anmelden. Dabei wird die Identität der betroffenen Personen gestohlen und Dritte geben sich als diese Personen aus. Zum digitalen Identitätsdiebstahl gehören auch Taten die man mit geringem IT-Wissen vollziehen kann, wie ein Fake Instagram Profile mit dem Namen/Bilder einer Fremden Person, wobei man ausgibt diese zu sein.
- **Daten-Leak:** Als Daten-Leak wird die Veröffentlichung von Nutzernamen und zugehöriger Passwörter bezeichnet. Sehr bekannte Beispiele hierfür sind WikiLeaks und die Panama Papers.

- **Collection #1 - #5:** Bestehen aus 2,2 Milliarden verschiedenen E-Mail-Adressen. Quelle: ‘https://www.pc-magazin.de/ratgeber/datenklau-aktuell-collection-1-betroffen-pruefen-have-i-been-pwned-3200357.html’
- **IDN-Homograph-Angriff:** Bezeichnet eine Methode des Spoofings, bei der Angreifer das ähnliche Erscheinen verschiedener Schriftzeichen dazu nutzt, Nutzern eine falsche Identität vorzutäuschen. Dazu werden oft Buchstaben verwendet, die sich in ASCII sehr ähnlich sehen. Beispiele sind das kyrillische kleine ‘a’ und das lateinische kleine ‘a’ oder einfacher ein 0 (Null) und ein O (oh). Dabei spielt es auch eine Rolle in welcher Schriftart die Buchstaben angezeigt werden. Die von Chrome und Firefox benutze Schriftart stellt diese gleich und damit ununterscheidbar dar (Tatsächlich funktionert dieser apple.com Link nicht mehr wie er sollte ind meiner Chrome Version 81). Theoretisch wird dem Nutzer jetzt apple.com als Internetseite angezeigt, die jedoch eine andere Seite im Hintergrund am laufen hat (hier die proof of concept Seite). Dies funktionert, da der Domainnamen mit kyrillischem ‘a’ von apple.com als ‘xn–80ak6aa92e.com’ registriert wird und im Browser lediglich als ‘apple.com’ angezeigt wird, was dazu führt, dass dem Nutzer eine falsche Identität vorgegaukelt wird und so auch falsche Vetrauen herrscht.
  Digitale Identitäten lassen sich nun erbeuten, indem man eine Seite baut die zB. Apples Seite 1:1 ähnlich aussieht jedoch das kyrillische ‘a’ in der Domain verwendet. Der Nutzer wiegt sich in vetrauter Umgebeung und versucht sich anzumelden, jedoch nun bei der falschen ‘xn–80ak6aa92e.com’ Adresse und der Angreifer erhält die Logindaten des Nutzers.