Aufgabe 1: Allgmeine Aussagen zur IT-Sicherheit

Aufgabe 1.1: Verteilte Systeme und Sicherheit

Aufgabe 1.2: Ursachen

Aufgabe 1.3: Angriffsformen

Aufgabe 2: Schutzziele

Aufgabe 2.1: Abgrenzung I

Aufgabe 2.2: Abgrenzung II

Aufgabe 2.3: Techniken

Aufgabe 3: Angreifemodell

Aufgabe 3.1: Angreifermodell

Unter einem Angreifermodell versteht man ein Modell mit Hilfe dessen man die Wirksamkeit eines Schutzmechanismus definieren kann. Abgebildet wird die Wirksamkeit auf die maximale Stärke eines Angreifers, vor dem der Schutz noch besteht. Angreifermodelle werden aufgestellt um die Wirksamkeit aktueller Schutzmechanismen zu vergleichen und zu analysieren. Zudem können sie herangezogen werden, um neue Schutzmechanismen zu entwickeln.

Die maximale Stärke eines Angreifers wird in unterschiedliche Kriterien aufgeteilt. Die Rolle, Verbreitung, das Verhalten und die Rechnerkapazität eines Angreifers.

Die Rolle es Angreifers beschreibt wie viel Wissen und Zugriff dem Angreifer zur Verfügung stehen, also ob dieser ein Insider (Produzent, Entwerfer...) oder Outsider(Benutzer...) ist.

Die Verbreitung des Angreifers beschreibt die Orte an denen Informationen von einem Angreifer abgegriffen werden können. Dies könnte als Beispiel das lokale Netzwerk oder alle in einem Land befindlichen Backbones sein.

Das Verhalten des Angreifers, sagt aus ob dieser passiv handelt, also nur Daten beobachten kann oder ob dieser aktiv in Systeme oder Datenflüsse eingreift. Ein passiver Angreifer könnte z.B jemand sein der Funksignale mithört oder aufzeichnet.

Die Rechenkapazität eines Angreifers ist bedeutend bei mathematischen bzw. kryptographischen Schutzmechanismen. Dessen Schutz basiert nämlich auf Problemen mit hinreichend langer Rechenzeit. Ein Angreifer, der über genügend Rechenkapazität verfügt kann diese Rechenzeit minimieren und somit den Schutz umgehen. Dies ist außerdem ein wichtiges Kriterium für die Schutzdauer eines Schutzmechanismus in Bezug auf die immer weiter zunehmende Rechenkapazitäten.

Aufgabe 3.2: Praxisbeispiel

Aufgabe 4: Passwortsicherheit

Aufgabe 4.1: Einfaches Hash-Verfahren

Aufgabe 4.2: Brute-Force-Angriff

Aufgabe 4.3: Time-Memory-Trade-Off

Aufgabe 4.4: Salting

Aufgabe 4.5: Dictionary-Attack