Aufgabe 1: Allgemeine Aussagen zur IT-Sicherheit

1. Verteilte Systeme und Sicherheit (Optional) – Welche Vor- bzw. Nachteile bzgl. der Sicherheit bietet ein verteiltes System gegenüber einem nicht-verteilten System?

Ein nicht-verteiltes System befindet sich lokal gesehen an einem Ort und benötigt kein Netzwerk um seinen Service zur Verfügung zu stellen. Es kann somit komplett abgeschottet werden und somit sind Angriffe über das Netzwerk nicht möglich. Der Nachteil hierbei ist, dass die Verfügbarkeit schnell verletzt werden kann, da eine physikalische Beeinträchtigung nur an einem Ort stattfinden muss. Das verteilte System hingegen ist gegen physikalische Beeinträchtigung an einem Ort besser geschützt, da dann nur eine Teil-Komponente des Systems ausfallen würde. Hingegen benötigt das verteilte System ein Netzwerk zur Kommunikation, was ein möglicher Angriffspunkt ist, um Vertraulichkeit und Integrität des Services zu beeinträchtigen.

2. Ursachen (Optional) – Nennen Sie die Ihrer Meinung nach drei häufigsten Ursachen für mangelnde IT-Sicherheit in Unternehmen.

- Kein Bewusstsein dafür / schlecht „aufgeklärt“
- Zu wenig Zeit, kein Fachpersonal
- Kein Geld

3. Angriffsformen (Optional) - Überlegen Sie sich, wie diese Systeme auf aktive oder passive Angriffe reagieren und welche Schutzziele dadurch bedroht sind. Für welche Angriffsart bzw. Angriffsarten sind die Systeme anfällig? Was wären mögliche Gegenmaßnahmen?

a) Dieses System ist vor allem gegen passive Angriffe anfällig. Hier kann sogar ohne Computerkenntnisse durch Beobachtung die erhöhte Anzahl der Essenslieferungen festgestellt werden. Steigt die Anzahl der Lieferungen, kann ein baldiger Angriff vorhergesagt werden, was eventuelle Überraschungsmomente abschwächt.
b) Das Problem besteht darin, dass beim Verbinden das Netzwerk mit der größten Signalstärke ausgewählt wird, sodass ein Angreifer ganz einfach an einem beliebigen

Ort einen weiteren WLAN-Access-Point mit der gleichen SSID einrichten kann. Alle Nutzer im nahen Umfeld verbinden sich dann mit dem Angreifer-AP. Dadurch kann der Netzwerkverkehr (problematisch bei Verzicht auf Verschlüsselung) mitgeschnitten werden. Access-Points ohne Namen sind auch nicht wesentlich besser. Es sollte lieber der Netzverkehr verschlüsselt werden, unter Umständen auch durch ein VPN.

Aufgabe 2: Schutzziele

1. Abgrenzung I (Pflicht, 5 Punkte) – Erläutern Sie die folgenden Schutzziele indem Sie sie jeweils voneinander abgrenzen:

a) **Anonymität:** Ein Nutzer kann einen Service/Dienst nutzen, ohne seine Identität zu offenbaren. (z.B. Web-Anonymisierer)
Pseudonymität: Ein Nutzer kann einen Service/Dienst nutzen, ohne seine wahre Identität zu offenbaren, in dem er sich als jemand anderes ausgibt. (z.B. Remailer)
Unbeobachtbarkeit: Ein Nutzer kann einen Service/Dienst nutzen, ohne dass jemand anderes dies nachvollziehen kann (z.B. anonymes Zahlungssystem)
b) **Vertraulichkeit:** Daten werden während der Übertragung geschützt, so dass nur Sender und Empfänger diese lesen können (z.B. durch Verschlüsselung)
Verdecktheit: Die Übertragung der Daten verläuft verdeckt, so dass nur Sender und Empfänger von der Übertragung wissen und Dritte nicht prüfen können, ob eine Übertragung stattfindet (z.B. Steganographie)

2. Abgrenzung II (Optional) – Erläutern Sie die folgenden Schutzziele indem Sie sie jeweils voneinander abgrenzen:

a) **Integrität:** Sicherstellung, dass Daten unverändert sind
Zurechenbarkeit: Benutzern kann das Senden/Empfangen von Daten nachgewiesen werden
b) **Verfügbarkeit:** Das System kann seinen Service innerhalb eines vereinbarten Zeitrahmens erfüllen
Erreichbarkeit: Das System kann erreicht werden bzw. es kann der Kontakt hergestellt werden wenn gewünscht.

3. Techniken (Optional) – Nennen Sie für jedes der obigen Schutzziele eine geeignete Technik, mit der das Schutzziel umgesetzt bzw. adressiert werden kann.

a) Anonymität, Pseudonymität, Unbeobachtbarkeit: Fake-Identitäten in Verbindung mit Proxy-Server.
b) Vertraulichkeit: Verschlüsselung in Kombination mit einem zentralen System, wo alle Nachrichten öffentlich (verschlüsselt) gespeichert und abgerufen werden können
c) Integrität, Zurechenbarkeit: Hashingverfahren der Daten und Signatur als Unterschrift
d) Verfügbarkeit, Erreichbarkeit: Gleiche Dienste mit gleichem Namen an mehreren Orten zur Verfügung stellen.

Aufgabe 3: Angreifermodell

1. Angreifermodell (Pflicht, 10 Punkte) – Was versteht man unter einem Angreifermodell und warum stellt man es auf? Welche einen Angreifer beschreibenden Kriterien werden in einem Angreifermodell berücksichtigt? Geben Sie zu jedem Kriterium auch die konkreten Ausprägungen an.

Das Angreifermodell definiert die maximal berücksichtigte Stärke eines Angreifers, gegen den ein Schutzmechanismus eines Systems gerade noch wirkt. Es wird verwendet, um zu zeigen, wie gut oder schlecht ein System in etwa gegen einen Angreifer geschützt ist. Das Modell wird in vier Teile unterteilt:

1. Rolle des Angreifers: Kann ein Benutzer, Außenstehender, Administrator usw. sein
2. Verbreitung des Angreifers: Die Orte, an denen Informationen gestohlen oder geändert werden können
3. Verhalten: Unterschied zwischen passivem Beobachten oder aktivem Eingreifen
4. Rechenkapazität: Wie viel Aufwand der Angreifer investiert/investieren kann

2. Praxisbeispiel (Optional) - Stellen Sie das Angreifermodell für das Abheben von Bargeld an Geldautomaten mit einer EC-Karte auf

1. Rolle: Sowohl intern können Administrator angreifen als auch extern etwa per Skimming
2. Verbreitung: Intern (Administrator) am Server, Extern direkt am Automaten
3. Verhalten: Ein Administrator könnte (bei unzureichenden Sicherheitsmaßnahmen) auch Datenverändernd eingreifen, ein Betrüger (Skimming) nur passiv.
4. Rechenkapazität: Unterschiedlich. Hängt wahrscheinlich von der möglichen „Beute“ ab.

Aufgabe 4: Passwordsicherheit

1. Einfaches Hash-Verfahren (Optional)

Das Kennwort wird gehasht gespeichert und zur Überprüfung wird das zu überprüfende Password gehasht und mit dem gespeicherten Hash verglichen. Es ist sicherer, da das wahre Passwort (meistens) nicht aus dem Hash zurückberechnet werden kann.

2. Brute-Force-Angriff (Optional)

$$t = \frac{52^8}{1000000} = 619d$$

3. Time-Memory-Trade-Off (Optional)

In Rainbow Tables warden zu Hashen die dazugehörigen Passwörter gespeichert. Diese muss einmal berechnet werden und dann kostet weniger Zeit zu einem Hash das dazugehörige Passwort zu finden, da die Table mehrmals für verschiedene Hashes verwendet werden kann. Diese Tabelle zu berechnen kostet aber viel Zeit und viel Speicherplatz. Somit lohnt sich dies nur, wenn mehrere Passwörter gefunden werden sollen.

4. Salting (Optional)

Rainbow Tables enthalten nutzen nur die Standard-Hashfunktion. Mit Salts wird allerdings die Hashfunktion leicht modifiziert bzw. die Eingabe zusätzlich abgeändert. Somit funktioniert die Rainbow Table nicht.

5. Dictionary-Attack (Optional)