Aufgabe 1: Allgemeine Aussagen zur IT-Sicherheit

(1) Ein verteiltes System bietet insofern eine erhöhte Sicherheit, als dass das System aus mehreren Teilkomponenten besteht, eine Infizierung oder ein Sicherheitsbruch einer Teilkomponente also nichtnotwendigerweise alle Teilkomponenten betrifft, was bei einem nicht-verteilten System der Fall wäre.
Ein Nachteil eines verteilten System gegenüber eines nicht-verteilten ist der erhöhte Wartungs-/Installationsaufwand, da mehrere Systeme offensichtlich einen größeren Ressourcenverbrauch bedeuten als einzelne, in sich geschlossene Systeme.

(2) DAU vor dem Bildschirm. Nutzung unsicherer Software/Systeme aufgrund von Komfortabilität jener Software/Systeme (sichere Systeme sind selten einfach und komfortabel benutzbar). Hohe Sicherheitsstandards verursachen häufig hohe Kosten, es existiert also ein Tradeoff zwischen Sicherheit und Machbarkeit/Finanzierbarkeit.

(3a) Da mehr Essen als normalerweise bestellt wird, ist der logische Schluss daraus, dass die Arbeitszeiten länger sind als sonst. Dies würde die Wahrscheinlichkeit von Fehlern durch Überarbeitung und/oder Übermüdung steigern.
Die Angreifbarkeit gegenüber Schadprogrammen oder Hacker aus dem Internet ist also erhöht.
Abgesehen davon könnte auch einer der zahlreichen Lieferanten Spionageabsichten haben. Beispielsweise könnte er versuchen mit einem WiFi-fähigen Gerät Funkverkehr abzuhören oder mit Schadsoftware ausgestattete USB-Sticks in Umlauf zu bringen.
In jedem Fall würde das Schutzziel der Vertraulichkeit also bedroht. Sollte ein Eindringen in das System per Schadsoftware gelingen, wäre ein verändernder Zugriff denkbar, sodass auch die Integrität und Verfügbarkeit als gefährdet einzustufen wäre.

(3b) Hier könnten alle drei Schutzziele beeinflusst werden. Bei einem öffentlichen, nicht verschlüsselten WLAN-Netz wäre es durchaus möglich, einen vorher manipulierten AP mit der gleichen SSID und entsprechender Schadsoftware auszustatten, auf die sich in der Nähe befindliche Clients dann automatisch verbinden.
Den über den AP laufenden Netzwerkverkehr könnte man dann loggen und später auswerten, damit wäre das Schutzziel der Vertraulichkeit verletzt.
Ebenfalls wäre eine Echtzeitmanipulation der Verbindung denkbar, indem man ankommende Daten in einen Cache lädt, diese verändern und erst dann zu dem Zielhost übermittelt.
Auch das Schutzziel der Verfügbarkeit ist gefährdet, da so einzelne Zielhost oder der komplette Datenverkehr blockiert werden könnten.

Aufgabe 2: Schutzziele

(1a) **Anonymität.** Bei der Anonymität können verschiedene Dienste vom Nutzer verwendet werden, ohne das dieser in irgendeiner Art und Weise seine Identität preisgibt. Selbst gegenüber dem Kommunikationspartner, beispielsweise beim Download einer öffentlichen Datei über eine verschlüsselte, nicht protokollierte Verbindung, bleibt die Identität der Nutzer unbekannt. Die Identifizierbarkeit des Nutzers darf also unter keinen Umständen gegeben sein. Eine Verschärfung

der Anonymität stellt die Unbeobachtbarkeit dar.
Unbeobachtbarkeit. Das Konzept der Unbeobachtbarkeit sichert dem Nutzer eines Dienstes oder einer Ressource zusätzlich zu, dass der Datenaustausch gegenüber Dritten unbeobachtbar bleibt, d.h. es kann nicht festgestellt werden, dass überhaupt kommuniziert wurde. Sowohl das Senden, als auch der eigentliche Datentransfer, sowie der Erhalt von Daten sind nicht festellbar.
Pseudonymität. Die Pseudonymität ist ein schwächeres Konzept im Vergleich zur Anonymität. Der Nutzer ist in seiner Identität gegenüber unbefugten Dritten und dem eigentlichen Kommunikationspartner anonym, jedoch ist der Nutzer über sein Pseudonym bestimmten Personen/Systemen bekannt. EIn Beispiel wäre der Abschluss eines Handels über eine entsprechende Plattform, bei der das Pseudonym des Nutzers als Käufer dem Verkäufer gegenüber bekannt gemacht wird.

(1b) **Vertraulichkeit.** Die Vertraulichkeit gewährleistet die Geheimhaltung von Daten während ihres Übertragungsprozesses zwischen den Kommunikationspartnern, beispielsweise mittels Verschlüsselung. Den Inhalt der Kommunikationsdaten kennen also lediglich die kommunizierenden Parteien.
Verdecktheit. Bei der Verdecktheit werden die zu übertragenden Daten versteckt übermittelt, sodass die Existenz der verdeckt übertragenden Daten ausschließlich den kommunizierenden Parteien bekannt ist. Ein einfaches, analoges Beispiel wäre ein Brief, auf dem zusätzlich zu einer belanglosen Nachricht eine weitere, verdeckte Botschaft mit Geheimtinte geschrieben wurde.

Aufgabe 3: Angreifermodell

NOCH BEARBEITEN!

3.1 Angreifermodell Definition: Das Angreifermodell beschreibt die Eigenschaften eines potentiellen Angreifers im Kontext eines worst-case Szenarios. Die Ausprägung der Eigenschaften wird als größtmöglich angenommen, jedoch in Abhängigkeit der maximalen Schutzmechanismen des Systems. Nutzen: Mögliche Systemschwachstellen bzw. mögliche Angriffspunkte werden erkannt und können behoben werden. Potentielle Risikobereiche werden identifiziert und somit das Bewusstsein zur besonderen Vorsicht geschärft.

Kriterien +Ausprägung:

1 Kriterium: Rollen des Angreifers

Ausprägung:(Außenstehender, Benutzer, Betreiber, Wartungsdienst, Produzent, Entwerfer ...), auch kombiniert

2. Kriterium: Verbreitung des Angreifers (Stellen im System, an denen der Angreifer Informationen gewinnen oder Systemzustände verändern kann)

Ausprägung:

3. Kriterium: Verhalten des Angreifers

Ausprägung: -passiv / aktiv,

-beobachtend / verändernd

4. Kriterium: Rechenkapazität des Angreifers

Ausprägung: - unbeschränkt: informationstheoretisch

- beschränkt: komplexitätstheoretisch