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.