Grundlagen der Systemsoftware

Übungsblatt 1 \* Gruppe G02-A \* Back, Behrendt, Stäger \* SoSe 2015

**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?

1. 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.
2. …

**Aufgabe 2: Schutzziele**

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

1. **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)

1. **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:

1. **Integrität:** Sicherstellung, dass Daten unverändert sind

**Zurechenbarkeit:** Veränderung von Daten kann einer Person zugeordnet werden

1. **Verfügbarkeit:** Das System kann seinen Service innerhalb eines vereinbarten Zeitrahmens erfüllen

**Erreichbarkeit:** ???

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

Siehe Beispiele in Klammern hinter den Begriffserklärungen.

Bitte überprüfen Sie, bevor Sie ein Aufgabenblatt abgeben:

* Rechtschreibung und Grammatik
* Nummer des Aufgabenblattes, Gruppennummer, Kleingruppen-Buchstabe und Name der Teilnehmer (siehe Kopfzeile und Fusszeile)
* Konvention für den Dateinamen. **G01B1A\_ANachname-BNachname-CNachname.pdf**bedeutet beispielsweise

Gruppe G01

Aufgabenblatt B1

Kleingruppe A

Teilnehmer ANachname, BNachname, CNachname