



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 nicht notwendigerweise 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.

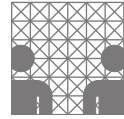
Den über den AP laufenden Netzwerkverkehr könnte man dann loggen und später auswerten, damit wäre das Schutzziel der Vertraulichkeit verletzt.

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 dass 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 feststellbar.

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 übertragenen 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.

(2a) **Integrität und Zurechenbarkeit.** Die Integrität von Daten beschreibt die Feststellbarkeit jeglicher Manipulation der Daten im Vergleich zu dem Originalzustand. Ist die Integrität von Daten zwischen Kommunikationspartnern gesichert, so kann jedwede Veränderung des Inhalts, also der Daten selbst, von den Kommunikationspartnern festgestellt werden und das unabhängig davon, ob die Daten vom Sender, vom Empfänger oder von einem Dritten verändert wurden.

Bei der Zurechenbarkeit hingegen wird nicht der Zustand einer Datei beschrieben, sondern die Sendung bzw. der Empfang der Daten. Hiermit kann das Verschicken oder das Erhalten einer Nachricht bewiesen werden.

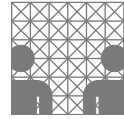
(2b) **Verfügbarkeit und Erreichbarkeit.** Das Schutzziel der Verfügbarkeit beschreibt die Möglichkeit der Nutzung eines bestimmten Dienstes zu jedem Zeitpunkt, an dem der Nutzer den Dienst nutzen möchte. Die Verfügbarkeit stellt damit eine Inanspruchnahme eines Dienstes zu jedem gewünschten Zeitpunkt dar. Die Erreichbarkeit hingegen garantiert nicht die ordnungsgemäße Nutzbarkeit eines Dienstes, sondern lediglich die Erreichbarkeit des Dienstanbieters (Ressourcen, Klienten, Menschen, ...).

(3) **Techniken.** Anonymität kann gewährleistet werden, wenn keine zur Identifizierung dienlichen Nutzerdaten während der Nutzung eines Dienstes protokolliert werden.

Unbeobachtbarkeit ist umsetzbar, wenn weder Nutzer noch Betreiber oder Dritte technisch feststellen können, dass zur Nutzungszeit eines Dienstes überhaupt eine Nutzung stattfindet.

Pseudonymität wird erreicht, wenn keine persönlichen, der Identifizierung dienlichen Daten protokolliert werden, sondern den Nutzern lediglich Pseudonyme zugeteilt werden, dessen Aktionen protokolliert werden.

Vertraulichkeit bei einem Datenaustausch ist realisierbar, wenn nur die Kommunikationspartner Zugriff auf den Inhalt der Daten haben, die Daten müssen dementsprechend verschlüsselt werden



um diesem Anspruch zu genügen.

Um Verdecktheit bei einer Kommunikation umzusetzen muss die eigentliche Nachricht versteckt werden, sodass die verdeckte Nachricht nicht feststellbar ist beim Datenaustausch. Bei analogen Medien wäre beispielsweise Geheimtinte denkbar, bei digitalen Medien das Einbetten der Nachricht in ein Bild, in Metadaten, in scheinbar freien Speicherplatz eines Speichermediums, ...

Die Integrität attestiert den Originalzustand von Daten. Dies kann mit einer Hashfunktion gewährleistet werden. Bei Sendung der Daten wird mittels einer Hashfunktion ein Hashwert erstellt, wird später auch nur ein einziges Bit des Inhalts geändert, ändert sich ebenfalls der Hashwert womit die Integrität der Daten verletzt ist.

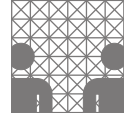
Die Zurechenbarkeit kann z.B. garantiert werden, wenn beim Senden oder Empfangen von Daten entsprechende Protokolle erstellt und automatisiert gesendet werden.

Die Verfügbarkeit eines Dienstes ist nur gewährleistet, wenn die Verfügbarkeit regelmäßig überprüft wird. Bei der Verfügbarkeit von Onlinediensten auf Servern beispielsweise werden regelmäßige Pings und andere Überprüfungssignale gesendet und dessen ordnungsgemäße Rücksendung erwartet. Antwortet ein Dienst nicht, ist seine Nicht-Verfügbarkeit sehr wahrscheinlich und entsprechendes Technikpersonal kann benachrichtigt werden. Um trotz erwartbarer Fehlermargen im Jahresmittel eine hohe Verfügbarkeit zu erreichen, können verteilte Systeme genutzt werden. Beispielsweise ist es möglich, zwei Server parallel bereit zu stellen wobei einer als Ausfallsicherung fungiert, die einspringt, sobald der erste Server nicht mehr ordnungsgemäß arbeitet.

Erreichbarkeit kann ebenso wie die Verfügbarkeit durch regelmäßige Überprüfungen und die Parallelbereitstellung sowie Verteilung von Diensten gewährleistet werden.

Aufgabe 3: Angreifermodell

(1) Das Angreifermodell beschreibt die Eigenschaften eines potentiellen Angreifers im Kontext eines worst-case Szenarios, also mit maximalen Möglichkeiten in der spezifischen Situation. Die Ausprägung der Eigenschaften wird also als größtmöglich angenommen, jedoch in Abhängigkeit der maximalen Schutzmechanismen des Systems. Das Angreifermodell beschreibt also die Situation eines starken Angreifers, bei dem die implementierten Schutzmechanismen aber noch Wirkung zeigen. Dies dient zur Charakterisierung der möglichen Angriffsszenarien sowie der Beschreibung der Schutzmechanismen. Die Aufstellung eines Angreifermodells macht insofern Sinn, als dass damit die aktuelle Sicherheitsarchitektur analysiert werden kann. Nach der Aufstellung ist ersichtlich, welche Angriffsszenarien maximal abgewehrt werden könnten, was die Einschätzung der aktuellen Sicherheit erleichtert und i.d.R. Handlungsbedarf respektive Verbesserungsmöglichkeiten aufzeigt, denn für entsprechend entdeckte Defizite kann dann eine Lösung erarbeitet werden. Mögliche Systemschwachstellen bzw. mögliche Angriffspunkte werden erkannt und können behoben werden. Zusätzlich dazu können potentielle Risikobereiche identifiziert werden, wodurch das Bewusstsein zur besonderen Vorsicht im Umgang mit diesen Bereichen geschärft wird. In einem Angreifermodell werden zunächst die Rollen des Angreifers abgebildet, dies umschreibt das Verhaltensmuster des Angreifers. Mögliche vorstellbare Ausprägungen wären Benutzer eines Dienstes, Betreiber eines Dienstes, Wartungsarbeiter eines Dienstes, Außenstehender mit Zugriff auf das Netzwerk usw. Kombinationen aus mehreren Ausprägungen sind denkbar. Hinzu kommt die Verbreitung des Angriffs, dies umschreibt die angreifbaren Lokalisationen des Systems, dies sind alle Stellen an denen der Angreifer das System manipulieren oder ausspähen kann. Des Wei-



teren wird das Verhalten des Angreifers beschrieben, welches passiv oder aktiv sein kann. Ein Ausspähen von Daten des Systems, also ein beobachtendes Verhalten, kann sowohl passiv als auch aktiv geschehen. Ein manipulatives Verhalten, also ein veränderndes Verhalten, kann nur aktiv passieren. Als letztes wird die Rechenkapazität des Angreifers genannt. Angenommen der Angreifer hätte unendliche Rechenkapazitäten zu Verfügung, dann wären herkömmliche Schutzmaßen nutzlos. Dies wird auch als informationstheoretischer Angriff bezeichnet. Die eher an der Realität orientierte Alternative ist bei dem Angreifer beschränkte Ressourcen zu vermuten, dies wäre ein komplexitätstheoretischer Angriff. Bei einem solchen Angriff hat der Angreifer endliche Rechenkapazitäten, sodass z.B. sehr komplexe Passwörter als sicher angenommen werden können, da die durchschnittliche Zeit zum Knacken der Passwörter bei ausreichender Komplexität schnell Hunderte oder Tausende von Jahren betragen kann.