Grundlagen der IT-Sicherheit

Übung 1

Gruppenmitglieder: Alexander Baumann
Marius Liedtke
Johannes Theiner

Semester: Wintersemester 2018/19
letzte Änderung: 28.10.2018

1 Grundlegende Begriffe

1.1 Benennen Sie den Unterschied zwischen Safety und Security. Geben Sie für beides jeweils zwei Beispiele aus dem IT-Bereich.

Der Unterschied zwischen Security und Safety ist der, dass die Security die Angriffssicherheit sowie Sicherheit vor Missbrauch darstellt, während die Safety die Betriebssicherheit darstellt.

Beispiele für Safety:

- Das automatische Abschalten von Betriebsanlagen (z.B. Roboter-Greifarm), bei Betreten des Raumes
- Ein Not-Aus-Schalter an technischen Anlagen
- Dateiberechtigungen zum Lesen/Schreiben/Ändern

Beispiele für Security:

- Ein Virenschutzprogramm
- Eine Passworteingabeaufforderung
- Eigentümerverwaltung zur Verhinderung von ungewollten Änderungen der Berechtigungen

1.2 Benennen Sie jeweils ein Gefährdungsbeispiel mit Begründung, das nicht unter den Begriff Security bzw. Safety fällt.

Fahrlässigkeit: Nichtbeachtung von Sicherheitsmaßnahmen, ungeeigneter Umgang mit Passwörtern.

Organisatorische Mängel: Fehlende oder unzureichende Regelungen, nicht erkannte Sicherheitsvorfälle.

Die Fahrlässigkeit des Benutzers sowie Organisatorische Mängel fallen weder in Safety noch in Security, da es sich weder um einen Angriffe von Außen, noch um einen Ausfallschutz relevanten Hintergrund handelt.

1.3 Erläutern Sie die Begriffe IT-Sicherheit und Informationssicherheit.

Die IT-Sicherheit bezeichnet die Sicherheit von soziotechnischen Systemen.

Dies umfasst die Sicherheit einer durch Technologie verknüpfte organisierte Menge von Menschen gegen Angriffe von außerhalb auf dieses verknüpfende Netzwerk (IT-System). Sie umfasst entsprechend nur die Sicherheit der technischen Systeme an sich.

Die Informationssicherheit umfasst neben der Sicherheit der IT-Systeme und der darin gespeicherten Daten auch die Sicherheit von nicht-elektronisch verarbeiteten Informationen, wie z.B. ein auf Papier notiertes Rezept, sowie die Organisation des Systems.

1.4 Grenzen Sie die Begriffe Schwachstelle, Bedrohung und Risiko voneinander ab.

Bedrohung: Ein Umstand, unter dem ein Schaden entstehen kann.

Risiko: Die Wahrscheinlichkeit, dass ein Schaden entsteht. Das Risiko läst sich auch berechnen als $Risiko = Schadenshöhe * Eintrittswahrscheinlichkeit$

Schwachstelle: Eine Schwachstelle ist ein sicherheitsrelevanter Fehler eines IT-Systems oder einer Institution.

1.5 Erläutern Sie, was sich hinter den ersten fünf Sicherheitsaspekten aus der Vorlesung verbirgt.

Authentizität: Der Sender einer Nachricht ist derjenige der er vorgibt zu sein.

Integrität: Der Inhalt einer Nachricht ist derjenige, den der Emittent tatsächlich verschickt hat.

Vertraulichkeit: Der Inhalt einer Nachricht bleibt vor dritten verborgen, also nicht semantisch erkennbar.

Verbindlichkeit: Das versenden einer Nachricht oder die Durchführung einer Aktion kann nachgewiesen werden.

Verfügbarkeit: Erreichbarkeit und Nutzbarkeit von Informationssystemen.

1.6 Worin unterscheiden sich insbesondere die Sicherheitsaspekte Integrität und Authentizität?

Die Integrität sorgt für Korrektheit von Daten und korrekte Ausführung von Systemen, während die Authentizität sicherstellt, dass die Daten vom korrekten Sender kommen und die Sender-Identität stimmt.

1.7 Was besagt das Recht auf informationelle Selbstbestimmung und in welchem Kontext ist es relevant? Geben Sie dafür ein Beispiel.

"Das Recht auf informationelle Selbstbestimmung ist im Recht Deutschlands das Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen".

Schutzbereich: Dieser ist weit gefasst. Es wird nicht unterschieden, ob mehr oder weniger sensible Daten des Einzelnen betroffen sind. Laut Bundesverfassungsgericht gäbe es keine belanglosen Daten, da im Zeitalter der Informationstechnologie auch scheinbar belanglose Daten wie ein einzelnes Datum zugeordnet werden kann.

Beispiel: Personenbezogene Daten, welche bei einer Registrierung auf einer Website angegeben werden müssen, dürfen ohne eine Genehmigung (z.B. per Zustimmung einer AGB) nicht an Dritte weitergegeben werden.

1.8 Worauf fußt das Bundesdatenschutzgesetz. Beschreiben Sie ganz kurz was damit geschützt werden soll?

Das Bundesdatenschutzgesetz fußt auf dem Volkszählungsurteil des Bundesverfassungsgerichts von 1983. Dieses etablierte das Grundrecht auf informationelle Selbstbestimmung als Ausfluss des allgemeinen Persönlichkeitsrechtes und der Menschenwürde.

Geschützte Daten: Geregelt wird der Umgang mit personenbezogenen Daten. Daten sind personenbezogen, wenn sie persönliche oder sachliche Verhältnisse einer natürlichen Person beschreiben. Dazu genügt es, wenn die Person nicht namentlich benannt wird, aber bestimmbar ist (beispielsweise: Telefonnummer, E-Mail-Adresse, IP-Adresse beim Surfen).

1.9 Erläutern Sie mit eigenen Worten die Begriffe Authentifizierung, Verifikation, Identifikation und Autorisierung und erläutern Sie den Zusammenhang zwischen den Begriffen.

Authentifizierung: ist der Nachweis (Verifizierung) einer behaupteten Eigenschaft einer Entität, die beispielsweise ein Mensch, ein Gerät, ein Dokument oder eine Information sein kann

Verifikation: ist der Nachweis, dass ein vermuteter oder behaupteter Sachverhalt wahr ist.

Identifikation: ist der Nachweis, dass ein vermuteter oder behaupteter Sachverhalt wahr ist.

Autorisierung: ist im weitesten Sinne eine Zustimmung oder Erlaubnis, spezieller die Einräumung von Rechten gegenüber interessierten Rechtssubjekten, gegebenenfalls als Nutzungsrecht gegenüber Dritten.

1.10 Was ist der Unterschied zwischen einer Identifikation und einer Verifikation?

Der Unterschied zwischen Identifikation und Verifikation ist, dass bei der Identifikation geprüft wird, um wen es sich handelt, jedoch bei der Verifikation geprüft wird ob ein Sachverhalt z.B. eine Identität der Wahrheit entspricht.

2 Identity Management

2.1 Was sind die Aufgaben des Identity Managements ?

- Daten über die einzelnen Entitäten speichern.
- Überprüfen ob eine Entität die ist für die sie sich ausgibt.
- Überprüfen ob eine Entität die Berechtigung hat auf einen bestimmten Teil des Systems zuzugreifen.

2.2 Erklären Sie den allgemeinen Prozess der Benutzerauthentifizierung.

Der Benutzer behauptet er hätte eine Zugangsberechtigung für ein System (etwa durch Angabe eines Nutzernames). Diese Behauptung wird vom System überprüft in dem das System den Benutzer verifiziert oder identifiziert. Kann diese Behauptung bestätigt werden ist der Benutzer authentifiziert und kann das System verwenden.

2.3 Auf welche Arten von Referenzdaten kann eine Authentifizierung basieren?

- Daten die nur der Nutzer wissen kann (PINs, Passwörter)
- Nachweise über den Besitz eines definierten Gegenstandes (Bankkarte, 2 Faktor)
- Biometrische Merkmale des Nutzers (Fingerabdruck, Stimme)

2.4 Zu welcher Authentifizierungsart gehört die Unterschrift bei einer EC-Karte.

Wird nur das aussehen der Unterschriften verglichen gehöhrt die Unterschrift zur Authentifikation durch Wissen, da es ausreicht zu wissen wie die Unterschrift aussieht um sich damit zu authentifizieren.

Würde zusätzlich die Dynamik der Schrift verglichen werden, gehöre die Unterschrift zur Authentifikation durch Merkmal.

2.5 Geben Sie ein Beispiel mit Begründung für eine statische und eine dynamische Modalität.

statisch: Venenmuster

- die meisten Menschen haben mindestens eine Hand
- verändert sich nicht
- ist einzigartig
- Spezielles Eingabegerät erforderlich

dynamisch: Tippverhalten

- kann sich im Laufe der Zeit durch Übung ändern
- ist nicht einzigartig

2.6 Erläutern Sie an Hand eines Beispiels warum die Eigenschaften second preiamge resistance und collsion resistance für Password Hashing von Bedeutung sind.

Ist der gewählte Hashing Algorithmus nicht second preiamge resistent kann es passieren das ein Nutzer sein Passwort ändert, aber trotzdem der gleiche Hash erzeugt wird und somit auch das alte Passwort noch funktioniert.

Hat der gewählte Hashing Algorithmus keine Kollisionsresistenz ist es sehr wahrscheinlich das für bekannte Hashes andere gültige Passwörter gefunden werden können.

2.7 Ist folgendes Bildungsgesetz eine gute Wahl für die Bildung von Passwörtern: 7 Zeichen aus [A-Z1-7!].

Dieses Bildungsgesetz erlaubt die Nutzung von 33 verschiedenen Zeichen. Somit hat ein solches Passwort eine Entropie von $\log_2(33^7) \approx 2^{35}$. Der Passwortcracker der Hochschule kann ein solches Passwort in unter einer Minute mit einem einfachen Brute-Force Angriff bestimmen.

2.8 Wie würden Sie ein Bildungsgesetz für Passwörter formulieren?

Passwörter sollten nicht mehr nach alten Regeln (mindestens 8 Zeichen, mindestens ein Sonderzeichen etc.) gebildet werden. Stattdessen sollten Sätze gebildet werden, die keinen Sinn ergeben müssen, aber trotzdem leicht zu merken sind. Wichtig ist nur das das gewählte Passwort lang genug ist, es sollte mit aktueller Rechenleistung mehrere Jahre dauern bis das Passwort per simplem Brute Force bestimmt werden kann.

2.9 Welche Maßnahmen würden Sie serverseitig ergreifen?

- Bei der Erstellung des Benutzer Accounts überprüfen ob:

  - das Passwort nicht in Wörterbüchern enthalten ist.
  - das Passwort nicht bereits aufgrund einer Sicherheitslücke eines anderen Dienstes veröffentlicht wurde.

- Passwort salten oder peppern.
- eine aktuell als sicher eingestufte Hash Funktion verwenden.
- Denn Benutzer andersweitig informieren wenn sich jemand mit dessen Account angemeldet hat.
- nach mehreren falschen Passworteingaben den Account temporär sperren.

3 Kerberos

3.1 Erläutern Sie den Begriff Single-Sign-On.

Single-Sign-On bedeutet, dass ein Benutzer nach einer einmaligen Authentifikation an einem Arbeitsplatz auf alle Rechner und Dienste, für die er lokal berechtigt ist, am selben Arbeitsplatz zugreifen kann, ohne sich jedes Mal neu anmelden zu müssen.

3.2 Was ist der Unterschied zwischen symmetrischer und asymmetrischer Verschlüsselung?

Bei der symmetrischen Verschlüsselung werden die Daten mittels eines geheimen Schlüssels ver- bzw. entschlüsselt. Der Schlüssel muss dabei sowohl Sender und Empfänger bekannt sein und zu diesem Zweck vorher persönlich ausgetauscht werden.

Die asymmetrische Verschlüsselung basiert auf der Verwendung eines zusammengehörenden Schlüsselpaares, wobei ein Schlüssel zur Ver- und einer zur Entschlüsselung genutzt wird. Beim Public Key Verfahren wird nun einer der Schlüssel veröffentlicht und kann von jedem Sender dazu genutzt werden, eine Nachricht an den Empfänger zu verschlüsseln. Nur der Empfänger, welcher in Besitz des zweiten privaten Schlüssels ist, kann die Nachricht dann entschlüsseln.

3.3 Worauf basiert Kerberos?

Ein zentraler Kerberos Server verwaltet die symmetrischen Schlüssel aller registrierten Benutzer durch ein symmetrisches Verfahren in älteren Versionen, ab Version 5 ist beides möglich und sorgt somit für deren Authentizität.

3.4 Wie erhält ein Benutzer das gemeinsame Geheimnis?

Möchte ein Benutzer A mit einem Benutzer B kommunizieren, fordert er vom Kerberos Server ein Ticket an. Dabei erzeugt der Kerberos Server einen zufälligen Sitzungsschlüssel, verschlüsselt diesen einmal mit dem Schlüssel von Benutzer A und einmal mit dem Schlüssel von Benutzer B und sendet beide Ergebnisse an Benutzer A. Benutzer A kann nun seinen Schlüssel nutzen um den Sitzungsschlüssel zu entschlüsseln und den mit dem Schlüssel von Benutzer B verschlüsselten Sitzungsschlüssel verwenden um mit Benutzer B Kontakt aufzunehmen. Somit werden nie unverschlüsselt Sitzungsschlüssel ausgetauscht und die Authentizität von Benutzer A gegenüber Benutzer B ist gewährleistet.

3.5 Welche Folgen hat es für die Verfügbarkeit einer IT-Infrastruktur, wenn in einer Kerberos Umgebung:

3.5.1 Der Authentication Server ausfällt

Wenn der Authentication Server ausfällt, kann der Client nicht auf seine bekannten Schlüssel zugreifen.

3.5.2 Der Ticket-Granting Server ausfällt

Wenn der Ticket-Granting Server ausfällt, kann kein Ticket erstellt werden, mit dem Sitzungsschlüssel ausgestellt werden.

3.5.3 Ein Server eines Dienstes ausfällt

Wenn ein Server eines Dienstes ausfällt, bekommt der Client ein Ticket, kann aber keine Verbindung zu dem Server aufbauen.