Hochschule Darmstadt

Zusammenfassung: 1. Semester

IT-Sicherheit

Leonhard Breuer
4. Januar 2024

Inhaltsverzeichnis

1 Grundlagen **5**

1.1 Die alltäglichen Probleme 5
1.2 By Design 5
1.2.1 Betriebssicherheit/Safety 5
1.2.2 Informationssicherheit/Security 6
1.2.3 Wechselwirkungen 6
1.3 Definitionen 7
1.4 Schutzziele 7
1.4.1 Übersicht 7
1.4.2 Vertraulichkeit 7
1.4.3 Integrität 8
1.4.4 Authenzität 8
1.4.5 Verbindlichkeit 8
1.4.6 Verfügbarkeit 8
1.4.7 Privatheit 8
1.5 IT-Sicherheit 8
1.5.1 Security-Policy 9
1.5.2 Gefahr 9
1.5.3 Bedrohung 9
1.5.4 Schwachstelle/Vulnerability 9
1.5.5 Gefährdung 9
1.5.6 Angriff 9
1.5.7 Angreifer 9

Kapitel 1

Grundlagen

1.1 Die alltäglichen Probleme

Täglich werden neue kritische Schwachstellen und Angriffe bekannt. Einige Beispiele:

- September 2020: Shitrix-Anriff
- Dezember 2018: Emotet (Banking Trojaner)
- Januar 2018: Meltdown and Spectre
- Oktober 2017: Return of Coppersmith Attack
- Juli 2015: Jeep Cherokee Hack (Zugriff auf kritische Fahrzeugfunktionen)
- Mitte 2014: Heartbleed (Fehler in OPENSSL)

1.2 By Design

Wegen der sich ständig weiterentwickelnden Technik müssen IT-Sicherheit und Datenschutz von Anfang an berücksichtigt werden.

Security by Design & **Privacy by Design**

1.2.1 Betriebssicherheit/Safety

Die Betriebssicherheit besagt, dass sich das Gerät/System konform seiner speziellen Funktion verhält bzw. das tut, was es soll. Die Safety umfasst auch einen Schutz aus Konsequenzen aus berechtigtem Handeln.

1.2.2 Informationssicherheit/Security

Die Security umfasst einen Schutz vor Konsequenzen aus vorsätzlichen und unberechtigen Handlungen. Gemäß dem **ISO / IEC 2382-1** - Standard gilt:

- Minimierung der Verwundbarkeit von Werten und Ressourcen
- Bewahren eines Systems vor Missbrauch

Informationssicherheit umfasst IT-Systeme (und darin gespeicherte Daten) und _nicht elektronisch verarbeitete Daten.

1.2.3 Wechselwirkungen

Hier einige Beispiele zu Wechselwirkungen von Safety und Security.

Security-Verletzungen können Safety gefährden Security Verletzungen können die Safety gefährden.

1. **Sicherheitsaspekt (Security):** Ein unbefugter Mitarbeiter oder Hacker hat Zugriff auf elektronische Patientenakten im Krankenhausinformationssystem (KIS). Dies könnte durch unzureichende Zugriffskontrollen, Schwachstellen in der Software oder unsichere Passwörter verursacht werden.
2. **Sicherheitsaspekt (Safety):** Die unbefugte Offenlegung oder Manipulation von Patientendaten könnte zu falschen medizinischen Entscheidungen führen. Ärzte könnten falsche Medikamente verschreiben oder lebenswichtige Informationen über Patienten könnten in falsche Hände geraten, was die Sicherheit der Patienten ernsthaft gefährdet.

Security-Maßnahme verletzt Safety Es ist möglich, dass eine zur allgemeinen Sicherheit eingeführte Maßnahme negative Einflüsse auf die Safety hat.

1. **Sicherheitsaspekt (Security):** Einführung biometrischer Zugangskontrollen im Labor, um den Zutritt zu sensiblen Bereichen zu reglementieren und unbefugten Zugriff zu verhindern.
2. **Sicherheitsaspekt (Safety):** Biometrische Systeme können jedoch zu Verzögerungen beim Zugang führen, insbesondere wenn Mitarbeiter dringend auf gefährliche Substanzen oder Notfälle reagieren müssen. Verzögerungen könnten die Sicherheit beeinträchtigen, wenn schnelle Reaktionen erforderlich sind.

Safety-Verletzung gefährdet Security Es ist möglich, dass durch eine Safety-Verletzung Sicherheitsrisiken entstehen.

1. **Sicherheitsaspekt (Safety):** Mitarbeiter erhalten keine angemessene Schulung im Umgang mit den Sicherheitssystemen im Labor, wie z.B. Brandschutzsystemen oder Notausgängen.

2. **Sicherheitsaspekt (Security):** Durch die mangelnde Schulung könnten Mitarbeiter unwissentlich Sicherheitssysteme umgehen oder falsch verwenden, was die Integrität der Sicherheitsinfrastruktur gefährden könnte. Unbeabsichtigte Auslösungen von Sicherheitsmaßnahmen durch ungeschultes Personal könnten zu Fehlalarmen führen und die tatsächliche Sicherheit des Labors beeinträchtigen.

1.3 Definitionen

Information Eine Information hat für den Empfänger i.d.R. einen Neuigkeitsgehalt. In der Informatik/IT-Sicherheit sind Informationen immer schützenswerte Güter.

Daten Repräsentation von Informationen z.B. als

- Bytefolge auf der Festplatte
- als Netzwerkpaket

Datensicherheit ist spezifischer als die Informationssicherheit.

IT-System ist ein dynamisches, technisches System, das Daten verarbeitet und speichert.

IT-Verbund ist die Gesamtheit von ... Objekten, die der Aufgabenerfüllung in einem Aufgabenbereich der Informationssicherheit dienen.

1.4 Schutzziele

1.4.1 Übersicht

- Vertraulichkeit (engl. confidentiality)
- Integrität (engl. entegrity)
- Authenzität (engl. authencity)
- Verbindlichkeit, Zurechenbarkeit (engl. accountability)
- Verfügbarkeit (engl. availability)
- Privatheit (engl. privacy)

1.4.2 Vertraulichkeit

Informationen dürfen nur für **autorisierten Personen** zugänglich sein.
Ein spezielles Problem der Vertraulichkeit sind *verdeckte Kanäle* und *Seitenkanalangriffe*.

verdeckte Kanäle

Verdeckte Kanäle sind Kommunikationswege zwischen Systemkomponenten, die unautorisierte Informationen übertragen, indem sie bestehende Kommunikationsmechanismen oder Ressourcen auf unkonventionelle Weise nutzen, oft in einem Versuch, Sicherheitsmechanismen zu umgehen.

Seitenkanalangriffe

Seitenkanalangriffe sind Angriffsmethoden, bei denen ein Angreifer Informationen aus einem kryptographischen System extrahiert, nicht durch direkte Analyse der verschlüsselten Daten, sondern durch Beobachtung von physikalischen Merkmalen wie Stromverbrauch, Laufzeit oder elektromagnetischer Strahlung während des Verschlüsselungsprozesses.

1.4.3 Integrität

Daten sind vollständig und **unverfälscht**.

1.4.4 Authenzität

Nachweisbarkeit der **Identität** eines Subjektes oder Objektes.

1.4.5 Verbindlichkeit

Ersteller von Daten kann diese Erstellung im Nachhinein **nicht abstreiten**.

1.4.6 Verfügbarkeit

Zugang und Befugnisse bleiben innerhalb der festgelegten Grenzen und werden nicht von unbefugten Dritten beeinflusst.

Berechnung der Verfügbarkeit

$$Verfuegbarkeit = \frac{Gesamtlaufzeit - Gesamtausfallzeit}{Gesamtlaufzeit}$$

1.4.7 Privatheit

Gewährleistung des informa4onellen Selbstbes4mmungsrechts und der Privatsphäre

1.5 IT-Sicherheit

Ziel der IT-Sicherheit ist: *Gewährleistung eines oder mehrerer Schutzziele für Daten, Dienste und Anwendungen*

1.5.1 Security-Policy

Eine Security-Policy besteht aus:

- Festlegung von Schutzzielen und Menge an Regeln.
- Festlegung der Maßnahmen zum Erreichen der Schutzziele.
- Festlegung von Verantwortlichkeiten und Rollen.

1.5.2 Gefahr

Eine Situation oder ein Sachverhalt führt zu negativen Auswirkungen. Es gibt jedoch keinen *zeitlicher*, *räumlichen* oder *personellen* Bezug.

1.5.3 Bedrohung

Eine Bedrohung ist eine **Gefahr** mit *zeitlichem*, *räumlichen* und *personellen* Bezug zu einem Schutzziel.

1.5.4 Schwachstelle/Vulnerability

Eine Schwachstelle ermöglicht das Umgehen der bestehenden Sicherheitsmaßnahmen durch technische oder organisatorische Mängel.

1.5.5 Gefährdung

Möglichkeit des *zeitlichen* oder *räumlichen* Zusammentreffens eines schützenswerten Gutes mit einer Schwachstelle.

1.5.6 Angriff

Ein Angriff ist ein unautorisierter Zugriff oder Zugriffsversuch auf auf IT-Systeme oder Informationen. Angriffe nutzen immer *Schwachstellen* aus.
Man unterscheidet zwei Kategorien von Angriffe:

aktiv Ziel ist *Informationsgewinnung*. Schutzziele *Vertraulichkeit*, *Privatheit*. Beispiel: Abhörung von Datenleitungen

passiv Ziel ist *Informationsveränderung*. Schutziele *Integrität*, *Authenzität*, *Verbindlichkeit* und *Verfügbarkeit*. Beispiel: Vortäuschen einer falschen Identität

1.5.7 Angreifer

Ein Angreifer ist eine *Person*, *System* oder eine *Personengruppe*, die einen Angriff ausführt.