Fachhochschule
Dortmund
University of Applied Sciences and Arts

Informationssicherheit – SoSe 2023
Terminologie

Prof. Dr. Holger Schmidt
holger.schmidt004[at]fh-dortmund.de

Fachhochschule Dortmund
Fachbereich Informatik
Professur für IT-Sicherheit, Informatik

Themen & Lernziele

Themen

- Informationssicherheit, IT-Sicherheit, Security vs. Safety
- Asset, CIA-Triad ergänzt um Authentifikation
- Schwachstelle/Verwundbarkeit
- Bedrohung, passiver/aktiver Angriff, Angreifertypen
- Risiko
- Sicherheitsmaßnahme

Lernziele

Die Studierenden sind in der Lage,

- selbständig Informationen über Schwachstellen zu sichten und zusammenzufassen.
- verschiedene Sicherheitsbegriffe zu differenzieren und zu erklären.
- grundlegende Terminologie der Informationssicherheit zu definieren und zu erklären.

IT-Sicherheit

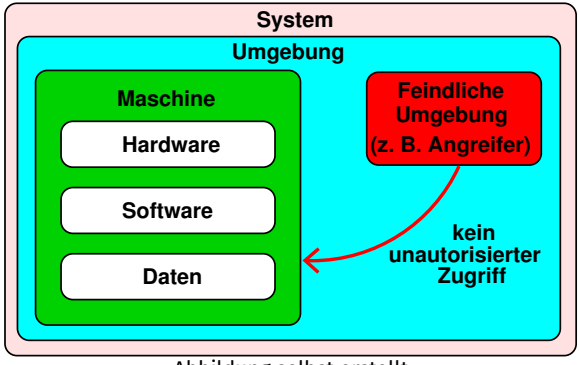


Abbildung selbst erstellt

- *System* $\triangleq$ *Maschine* + *Umgebung*
  nach Zave und Jackson, 1997
- Hier: **IT-Sicherheit** $\triangleq$ Security
- IT-Sicherheit ist eine **Eigenschaft des Systems**
  (und nicht *nur* z. B. der Software).

Informationssicherheit

- IT-Sicherheit bezieht sich auf Informationstechnologie
- IT-Sicherheit ist ein **Teilgebiet** der Informationssicherheit
- Informationssicherheit betrachtet **zusätzlich** u. a.
  - **Menschen**
  - Organisatorische Prozesse
  - Physische Sicherheitsmaßnahmen
- „Erweiterter Systembegriff“

Schützenswerte Ressource / Asset

Ein **asset** ist das was wir schützen wollen.

„…an asset which has a value requiring appropriate protection …“
ISO/IEC 27000, 2018

- Informationen, z. B. Datenbanken, Quellcode
- Materielle Güter, z. B. Hardware, Maschinen, Räume
- Immaterielle Güter, z. B. Reputation
- Personen, z. B. Kunden, Mitarbeiter

Schutzziele

„preservation of confidentiality …, integrity …and availability …of information“ ISO/IEC 27000, 2018

- **CIA-Triad**
- Wir betrachten Schutzziele allgemeiner als in der ISO/IEC 27000, 2018: **asset statt information**
- Anhaltende Debatte über eine **Erweiterung** der CIA-Triad

CIA-Schutzziel Vertraulichkeit / Confidentiality

„property that information is not made available or disclosed to unauthorized individuals, entities, or processes“ ISO/IEC 27000, 2018

- Ziel: Beschränkung und Kontrolle des Zugriffs auf Informationen für autorisierte Personen, Instanzen und Prozesse
- Bedrohungen: z. B. Abhören von Finanzstatus beim Internetbanking
- Vorfall, z. B. : Auslesen von 900 Sozialversicherungsnummern von Servern des kanadischen Finanzamtes basierend auf Heartbleed[1]
- Technische Maßnahmen, z. B. :
  - Zur Wahrung der Vertraulichkeit bei Speicherung und Transfer sensibler Informationen werden **Verfahren zur Verschlüsselung** eingesetzt.
  - **Zugangskontrollen** und **Regulierung der Informationsflüsse** dienen zum Schutz vor unautorisierten Zugriffen.

[1] https://www.heise.de/security/meldung/Heartbleed-Datendiebstahl-beim-kanadischen-Finanzamt-2169832.html, aufgerufen am 28. Juni 2023

CIA-Schutzziel – Integrität / Integrity

„property of accuracy and completeness“ ISO/IEC 27000, 2018

- Ziel: Wahrung von Vollständigkeit und Korrektheit von Informationen bzw. Daten und Systemen
- Bedrohungen: z. B. Manipulation von Quellcode
- Vorfall, z. B. : Ransomware verschlüsselt Daten auf Bezahlterminals der Stadtbahn in San Francisco[2]
- Technische Maßnahmen, z. B. :
  - Geregelte und funktionsfähige **Berechtigungen** und **Zugangskontrollen**
  - Möglichkeiten der Manipulation werden durch präzise funktionale Einschränkung bzw. Modularisierung reduziert.
  - **Redundanz** (Backup, RAID)
  - Datenveränderungen können z. B. mittels **Hashfunktionen** ermittelt werden.

[2] https://heise.de/-3506080, aufgerufen am 28. Juni 2023

CIA-Schutzziel – Verfügbarkeit / Availability

Fachhochschule Dortmund
University of Applied Sciences and Arts

„property of being accessible and usable on demand by an authorized entity“ ISO/IEC 27000, 2018

- Ziel: Sicherstellung des Zugriffs durch autorisierte Instanzen und somit die Gewährleistung von Erreichbarkeit und damit verbundener Produktivität
- Bedrohungen: z. B. gezielte Angriffe, **Naturgewalten**, **technische Fehler**
- Vorfall, z. B. : Störung von Telekom-Routern über Fernwartungs-Port[3]
- Technische Maßnahmen, z. B. :
  - Intrusion Detection Systeme
  - Firewalls
  - Lastverteilung

[3] https://www.heise.de/security/meldung/Grossstoerung-bei-der-Telekom-Angreifer-nutzten-Luecke-und-Botnetz-Code-3507088.html, aufgerufen am 28. Juni 2023

Erweitertes Schutzziel Authentizität / Authenticity

Fachhochschule Dortmund
University of Applied Sciences and Arts

„provision of assurance that a claimed characteristic of an entity is correct“ ISO/IEC 27000, 2018

- Ziel: Gewährleistung von Echtheit, Glaubwürdigkeit und Überprüfbarkeit von Objekten und Subjekten
- z. B. Fälschung von biometrischen Merkmalen, Erraten von Passwörtern, Diebstahl von Smartcards
- Vorfall, z. B. : Überwindung des iPhone 5S Fingerabdrucksensors mithilfe von Attrappen[4]
- Technische Maßnahmen, z. B. :
  - **Passwörter**
  - Biometrische Merkmale, Smartcards

[4] https://youtu.be/HM8b8d8kSNQ, aufgerufen am 28. Juni 2023

Bedrohung / Threat

Eine **Bedrohung** ist das wogegen wir schützen wollen.

„potential cause of an unwanted incident, which can result in harm to a system or organization“ ISO/IEC 27000, 2018

- Ausnutzung einer oder mehrerer Verwundbarkeiten eines Systems, um eine **Verletzung der Schutzziele** zu erreichen
- „…the enemy knows the system …“ nach Shannon, 1949
- **Bedrohungsmodell** betrachtet entsprechend Asset, Schutzziele, Verwundbarkeit und zusätzlich (insb. feindliche) Umgebung, z. B. **Angreifer** und dessen **Fähigkeiten** und **Zielen**

Klassifikation von Bedrohungsfaktoren

- **Höhere Gewalt**
  Blitzschlag, Feuer, Überschwemmung, Erdbeben, Demonstration, Streik
- **Fahrlässigkeit**
  Irrtum, Fehlbedienung, unsachgemäße Behandlung
- **Vorsatz**
  Manipulation, Einbruch, Hacking, Vandalismus, Spionage, Sabotage
- **Technisches Versagen**
  Stromausfall, Hardware-Ausfall, Fehlfunktionen
- **Organisatorische Mängel**
  Unberechtigter Zugriff, Raubkopie, ungeschultes Personal

Schwachstelle / Weakness und Verwundbarkeit / Vulnerability I

Eine **Verwundbarkeit** ist eine ausnutzbare **Schwachstelle** im System.

„weakness of an asset or control … that can be exploited by one or more threats“ ISO/IEC 27000, 2018

- Eine Schwachstelle (**weakness**) ist eine Schwäche eines Systems bzw. eine Situation oder Stelle (typischerweise ein Asset, eine Sicherheitsmaßnahme oder eine Funktionalität), an der ein System verwundbar ist.
- Schwachstellen können z. B. natürlicher (z. B. die Anfälligkeit für Naturkatastrophen), physischer (z. B. Einbruch in Serverraum) oder menschlicher (z. B. durch den Menschen verursachte Fehler) Art sein.

Schwachstelle / Weakness und Verwundbarkeit / Vulnerability II

- Häufig entstehen Schwachstellen durch **unsachgemäße Systemnutzung**, **Softwarefehler** oder **unsichere Kommunikationsverbindungen**.
- Verwundbarkeit (**vulnerability**) ist eine ausgenutzte Schwachstelle, über die z. B. sicherheitsrelevante Systemdienste umgangen, getäuscht oder unautorisiert modifiziert werden können.
- Gängige Softwarefehler, die zu Verwundbarkeiten führen, sind z. B. nicht korrekt abgefangene **Pufferbereichsüberläufe** aufgrund von Eingaben.

Eine Auswahl bekannter Schwachstellen

CVE-2016-2118

CVE-2017-5754

CVE-2017-5753,
CVE-2017-5715

CVE-2015-3197

CVE-2017-17688,
CVE-2017-17689

CVE-2016-5195

Quelle der Logos: https://commons.wikimedia.org/wiki/Category:Security_vulnerability_logos, aufgerufen am 28. Juni 2023

Angriff / Attack

„attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset“ ISO/IEC 27000, 2018

- Realisierung einer Bedrohung
- Sowohl ein nicht autorisierter Zugriff als auch ein Zugriffsversuch auf ein System werden als Angriff bezeichnet.
- Aufteilung in **passive** und **aktive Angriffe**.
- **Passive Angriffe** beschreiben eine unautorisierte Informationsgewinnung und können z. B. einen Verlust der **Vertraulichkeit** zur Folge haben.
- **Aktive Angriffe** umfassen die unautorisierte Modifikation von Datenobjekten und richten sich vor allem gegen die **Integrität** und **Verfügbarkeit** von IT-Systemen.

Hackers

- Begriff eingeführt durch Levy, 1984
- **Hackerethik**, z. B. vom CCC[5] bzw. als 35C3 Video[6]
- **White Hat Hacking bzw. Ethical Hacking bzw. Penetration Testing**
- Organisiert, z. B. jährliche Treffen
  - DEF CON Convention[7]
  - Chaos Communication Congress[8]
  - Black Hat Conference[9]

[5] https://www.ccc.de/de/hackerethik, aufgerufen am 28. Juni 2023
[6] https://media.ccc.de/v/35c3-10011-hackerethik_-_eine_einfuhrung, aufgerufen am 28. Juni 2023
[7] https://defcon.org/, aufgerufen am 28. Juni 2023
[8] https://events.ccc.de/congress/, aufgerufen am 28. Juni 2023
[9] https://www.blackhat.com/, aufgerufen am 28. Juni 2023

Vergleich Black/Grey/White Hat Hacker

		Hacker Typen		
		Black Hat	**Grey Hat**	**White Hat**
Ver-	**identifizieren**	Bedingungslos (ggf. illegal!)	Bedingungslos (ggf. illegal!)	Nur mit Erlaubnis
wund-	**ausnutzen**	Bedingungslos (illegal!)	Nur mit Erlaubnis	Nur mit Erlaubnis
barkeit	**veröffentlichen**	Öffentlichkeit, mit Exploit	Nur Hersteller, Problembehebung gegen Bezahlung	Nein, bis Problem behoben
Motivation		eigener Vorteil, Schädigung Dritter	Risikoreduktion, Bezahlung	
Fähigkeiten		Technisch sehr versiert		

Weitere Differenzierung von Angreifer-Typen I

- Differenzierung zwischen **internen** und **externen Angreifern**.
  - Interne Angreifer (auch Innentäter) sind meist Angestellte eines Unternehmens oder extern beauftragte Personen, die über eine Vielzahl unterschiedlicher Interna verfügen und dieses Wissen gezielt für einen Angriff ausnutzen können.
  - Externe Angreifer sind vor allem durch die Zunahme der Vernetzung und Öffnung von Systemen zu einer großen Bedrohung erwachsen. Externe Angriffe unterliegen zusätzlich einer steigenden Kriminalisierung.

- **Skript Kiddie**
  Stereotyp für einen Angreifer, der meist über geringes technisches Hintergrundwissen, dafür aber viel Zeit verfügt. Angreifer sind häufig Jugendliche und nutzen vor allem **frei verfügbare Exploits** zum Angriff auf Computersysteme.

Weitere Differenzierung von Angreifer-Typen II

- **Wirtschaftsspionage**
  Sehr hoch technisierter Angreifer, der mit großem Aufwand gezielte Angriffe auf Unternehmen durchführt. Ziel ist meist die Erlangung vertraulicher Informationen. Häufig handelt es sich um einen sog. **APT** (Advanced Persistent Threat), der sich durch die längerfristig andauernde Bedrohung auszeichnet.

- **Geheimdienste**
  Die Veröffentlichungen des ehemaligen NSA-Mitarbeiters Edward Snowden zeigen eine **flächendeckende Überwachung** internationaler Telekommunikationsverbindungen durch Geheimdienste. Häufig stellt diese Überwachung gleichzeitig eine Wirtschaftsspionage dar.

Passive Angriffe – Beispiele

- **Sniffing-Angriffe** (auch eavesdropping und wiretapping)
  Mitschneiden von Datenverkehr oder Abhören von Telefonleitungen zum Ausspähen von internen Informationen, so beispielsweise Passwörtern.

- **Portscans**
  Ermittlung geöffneter Ports für Services. Diese können ggf. im weiteren Verlauf eines Angriffs gezielt ausgenutzt werden.

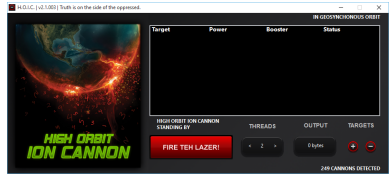
- **Idle-Scans**
  Dienen auch der Ermittlung aktiver Dienste, ohne dabei die angreifende IP-Adresse bekanntzugeben.

Portscan mittels Nmap unter Linux – Foto selbst erstellt

Aktive Angriffe – Beispiele I

- **Spoofing-Angriffe**
  Spoofing- bzw. Maskierungsangriffe basieren auf der Vortäuschung einer falschen Identität. Dies kann beispielsweise eine falsche E-Mail-Adresse oder gezielt angepasste MAC-Adresse sein.

- **Denial-of-Service-Angriffe** (DoS)
  Angriff zur Einschränkung der Verfügbarkeit von Systemen bzw. Diensten. Hierzu kann z. B. der Netzwerkverkehr bewusst überlastet und somit eine normale Erreichbarkeit verhindert werden.



High Orbit Ion Cannon für DoS-Angriffe[10] – Foto selbst erstellt

[10] https://sourceforge.net/projects/high-orbit-ion-cannon/, aufgerufen am 28. Juni 2023

Aktive Angriffe – Beispiele II

- **Man-in-the-middle-Angriffe**
  Angreifer befindet sich zwischen zwei Kommunikationspartnern und ist in der Lage den Datenverkehr einzusehen und zu manipulieren. Ein physischer Zugang ist hierfür nicht (mehr) erforderlich.

- **Pufferüberlauf** (buffer overflow)
  Ausnutzung von Programmierfehlern, die aufgrund einer unzureichenden Prüfung von Eingaben einen Überlauf zur Folge haben und somit die Ausführung von Schadcode in fremden Speicherbereichen ermöglichen.

- **Social Engineering**
  Nicht-technische Angriffe, bei denen ein Angreifer ein Opfer z. B. zur Preisgabe sensibler Informationen bewegt, indem er eine falsche Identität bzw. Rolle vorgibt (z. B. Systemadministrator des Unternehmens) und um Unterstützung bittet.

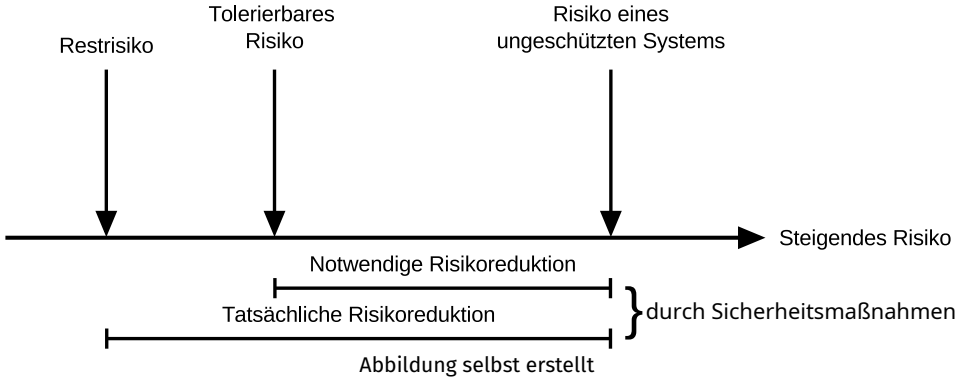
Risiko / Risk I

„effect of uncertainty on objectives“ ISO/IEC 27000, 2018

Anmerkung: **„Information security risk is associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization.“** ISO/IEC 27000, 2018

- Das Risiko einer Bedrohung beschreibt die **Eintrittswahrscheinlichkeit** (relative Häufigkeit) eines Schadensereignisses und die **Höhe eines potentiellen Schadens**.
- Das Bedrohungsrisiko ist stark vom darunterliegenden **Angreifermodell** abhängig, welches potentielle Angreifer nach Fähigkeiten und Zielen charakterisiert (z. B. Kenntnisse, Ressourcen und Budget).

Risiko / Risk II



- In Abhängigkeit zu schützender Assets kann eine Aussage zum **Schutzbedarf** entwickelt werden.
- **Wirtschaftlichkeit** von Informationssicherheit

Sicherheitsmaßnahme / countermeasure bzw. control I

„measure that is modifying risk“ ISO/IEC 27000, 2018

- Ziel: **Risikoreduktion (Härtung)**
- **Abschreckung** durch Strafen (Recht)
- **Verhinderung** bzw. **Prävention** durch
  - **technische** Sicherheitsmaßnahmen, z. B. Einsatz von Verfahren zur Verschlüsselung
  - **nicht-technische** Sicherheitsmaßnahmen, z. B. Passwortrichtlinien

Sicherheitsmaßnahme / countermeasure bzw. control II

- Falls Prävention nicht gelingt oder nicht möglich, dann zumindest **Erkennung**:
  - Angriffsversuche erkennen (schwierig bei passiven Angriffen) und stoppen (kein Schaden)
  - Angriffe erkennen (Schaden möglich)
  - Schwierig bei passiven Angriffen
  - **Reaktion** erforderlich
  - **Wiederherstellung** bei Schäden
- **Mehrstufiges Schichtenkonzept**

Zusammenfassung

Zusammenfassung

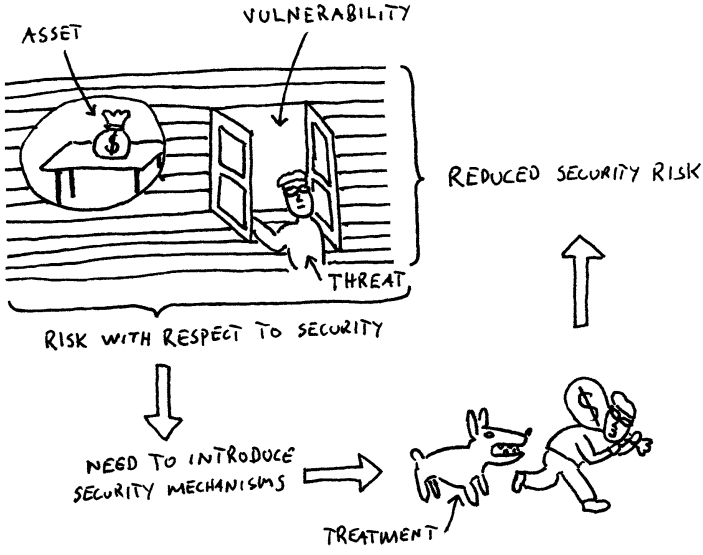


Abbildung 6.2 aus Lund et al., 2010

Weiterführende Literatur

Weiterführende Literatur

- *IT-Sicherheit – Konzepte - Verfahren - Protokolle*, Kapitel 1 von Eckert (2023)
- *Security Engineering: A Guide to Building Dependable Distributed Systems*, Kapitel 1 von Anderson (2020)

Literatur

- Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems* (3. Aufl.). John Wiley & Sons Inc. https://www.cl.cam.ac.uk/~rja14/book.html (siehe S. 33).
- Eckert, C. (2023). *IT-Sicherheit: Konzepte - Verfahren - Protokolle* (11. Aufl.). De Gruyter Oldenbourg. (Siehe S. 33).
- ISO/IEC 27000. (2018). ISO/IEC 27000: Information technology – Security techniques – Information security management systems – Overview and vocabulary. (Siehe S. 7–13, 15, 18, 26, 28).
- Levy, S. (1984). *Hackers: Heroes of the Computer Revolution*. Doubleday. (Siehe S. 19).
- Lund, M. S., Solhaug, B., & Stølen, K. (2010). *Model-Driven Risk Analysis: The CORAS Approach* (1st). Springer Publishing Company, Incorporated. (Siehe S. 31).
- Shannon, C. (1949).Communication Theory of Secrecy Systems. *Bell System Technical Journal*, *28*(4), 656–715 (siehe S. 13).
- Zave, P., & Jackson, M. (1997).Four dark corners of requirements engineering. *ACM Transactions on Software Engineering and Methodology*, *6*(1), 1–30 (siehe S. 5).