Fachhochschule
Dortmund
University of Applied Sciences and Arts

Informationssicherheit – SoSe 2023
Recht & Standards

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

Fachhochschule Dortmund
Fachbereich Informatik
Professur für IT-Sicherheit, Informatik

Themen & Lernziele

Themen

- Rechtliche Rahmenbedingungen in Deutschland
- Europäische Datenschutzgrundverordnung
- Einleitung Standards und Best Practices
- ISO/IEC 15408:2022 und ISO/IEC 18045:2022 aka Common Criteria

Lernziele

Die Studierenden sind in der Lage,

- Informationssicherheit im Kontext der deutschen IT-Sicherheitsgesetze zu erklären.
- grundlegende Inhalte der europäischen Datenschutz-Grundverordnung wiederzugeben und anzuwenden.
- die Bedeutung von Standards für die Informationssicherheit einzuschätzen.
- Grundlagen der Common Criteria zu erklären sowie Bedrohungs- und Schwachstellenanalysen durchzuführen.

Rechtliche Rahmenbedingungen in Deutschland

BSI-Gesetz

„Sicherheit in der Informationstechnik im Sinne dieses Gesetzes bedeutet die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen

1. in informationstechnischen Systemen, Komponenten oder Prozessen oder
2. bei der Anwendung von informationstechnischen Systemen, Komponenten oder Prozessen.“

Legaldefinition der IT-Sicherheit im Gesetz zur Errichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) (**BSI-Gesetz**) vom 14. August 2009 (BGBl. I S. 2821)[1]

[1] http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl109s2821.pdf, aufgerufen am 18. April 2023

IT-Sicherheitsgesetz 2.0

- **Weiterentwicklung** des BSI-Gesetzes[2]
- Zuletzt geändert am 21.05.2021 (BGBl. I S. 1122) durch zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (**IT-Sicherheitsgesetz 2.0**)[3]
- **Kritische Infrastruktur** im Fokus: Betreiber nachweispflichtig bzgl. Einhaltung von Standards, Meldepflicht bei Störungen

[2] https://www.bsi.bund.de/DE/Das-BSI/Auftrag/BSI-Gesetz/bsi-gesetz_node.html, aufgerufen am 18. April 2023

[3] https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl121s1122.pdf, aufgerufen am 18. April 2023

Datenschutz in Europa

Datenschutz – Einleitung

- Grundlage bildet das **Recht auf informationelle Selbstbestimmung** (Volkszählungsurteil des Bundesverfassungsgerichtes von 1983[4]).
- Ziel ist der **Schutz des Persönlichkeitsrechts** und somit **personenbezogener Daten**.
- Jeder Mensch soll **selbst über die Verwendung und Preisgabe ihn betreffender Daten entscheiden** können.
- Geschützt werden also nicht Daten, sondern die **Freiheit** der Menschen, selbst zu entscheiden, wer was wann und bei welcher Gelegenheit über sie weiß.

Vgl. Reinhard et al., 2007

[4] https://web.archive.org/web/20101116085553/http://zensus2011.de/fileadmin/material/pdf/gesetze/volkszaehlungsurteil_1983.pdf, aufgerufen am 18. April 2023

Datenschutz – Gesetzgebung in Europa

- Die Europäische **Datenschutz-Grundverordnung (DS-GVO)**[5] ist nach der Übergangsphase von zwei Jahren ab dem 25. Mai 2018 europaweit geltendes Recht.
- Die DS-GVO löst eine seit 1995 geltende EU-Richtlinie 95/46/EG[6] ab und ersetzt nationale Datenschutzgesetze (z. B. Bundesdatenschutzgesetz (BDSG)[7]) durch **unmittelbar geltendes EU-Recht**.

[5] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32016R0679, aufgerufen am 18. April 2023
[6] http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:31995L0046, aufgerufen am 18. April 2023
[7] https://web.archive.org/web/20180401002313/https://www.gesetze-im-internet.de/bdsg_1990/, aufgerufen am 18. April 2023

Personenbezogene Daten nach DS-GVO

Personenbezogene Daten sind nach Art. 4 DS-GVO alle Daten „…die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen …“[8].

- **Identifikation** passiert durch „…direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen …“[8].
- Solche **Kennungen** müssen „…Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person …“[8] sein.
- Beispiele: Namen, Adressen, Gesundheitsdaten, Kontonummern, IP-Adressen

[8] Artikel 4 in http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32016R0679, aufgerufen am 18. April 2023

Geldbußen und Zertifizierung nach DS-GVO

Fachhochschule Dortmund
University of Applied Sciences and Arts

- Deutliche Erhöhung des Rahmens für **Geldbußen**: bis zu 20.000.000€ bzw. bei Unternehmen bis zu 4% des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres
- Art. 42 und 43 DS-GVO legen rechtlichen Grundstein für **europäisch einheitliche Akkreditierungs- und Zertifizierungsverfahren**, die dazu dienen, die Einhaltung der DS-GVO bei Verarbeitungsvorgängen nachzuweisen.

Grundsätze der DS-GVO I

Art. 5 Abs. 1 DSGVO beschreibt „Grundregeln“ für die Verarbeitung von personenbezogenen Daten DSGVO:

- Rechtmäßigkeit der Verarbeitung (konkretisiert in Art. 6 DS-GVO: **Verbot mit Erlaubnisvorbehalt, Rechtsgrundlage, Einwilligung**)
- Verarbeitung nach Treu und Glauben: **Redlichkeit, Anständigkeit**
- Transparenz: **Auskunftsrecht** nach Art. 15 Abs. 1 DS-GVO, **data protection by design**[9]**, data protection by default**
- **Zweckbindung**

[9] ISO 31700, https://www.iso.org/standard/84977.html, aufgerufen am 18. April 2023

Grundsätze der DS-GVO II I

- **Integrität und Vertraulichkeit** (konkretisiert in Art. 32 DS-GVO: geeignete technische und organisatorische Maßnahmen)
- Richtigkeit der Datenverarbeitung (konkretisiert in Art. 16 DS-GVO: **Unverzügliche Berichtigung**)
- **Datenminimierung** (früher „Datenvermeidung und Datensparsamkeit“ nach BDSG)
- **Speicherbegrenzung** (zeitlich, Archivierung ausgeschlossen)

IT-Sicherheit in der DS-GVO

- Schutzbedarf richtet sich nach
  - **Stand der Technik**,
  - **Umsetzungskosten**,
  - **Eintrittswahrscheinlichkeit** und
  - **Risiko**

  „…für die Rechte und Freiheiten natürlicher Personen …“[10].
- „…geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten …“[10]
- Konkret verpflichtend: **Pseudonymisierung, Verschlüsselung, Backups**

[10] Artikel 32 in http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32016R0679, aufgerufen am 18. April 2023

IT-Sicherheit in der DS-GVO – PDCA-Zyklus

Fachhochschule Dortmund
University of Applied Sciences and Arts

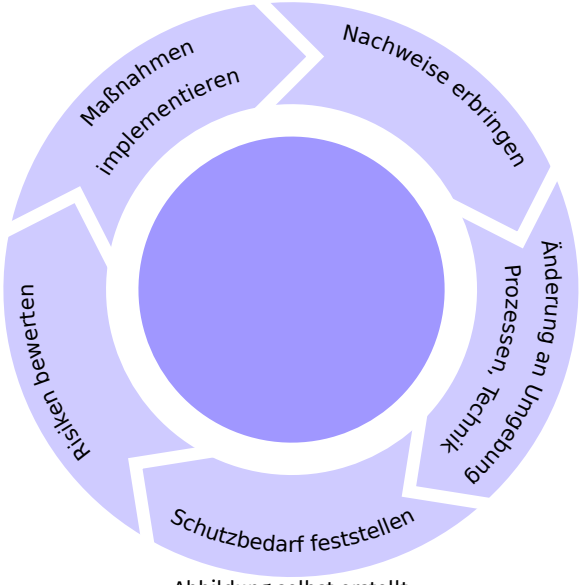


Abbildung selbst erstellt

Standards und Best Practices

Einleitung

- Gewährleistung von **Mindeststandards** und **Vergleichbarkeit** hinsichtlich Informationssicherheit durch Standards und Best Practices.
- Bereitstellung von **Vorgehensweisen** zur effizienten Absicherung von Systemen und Infrastrukturen.
- Gewährleistung der Einhaltung etwaiger gesetzlicher und regulatorischer Anforderungen.
- Nachweis durch **Zertifizierung** von z. B. Unternehmen und Produkten.

Beispiele

- **Standards**
  - Common Criteria for Information Technology Security Evaluation (Common Criteria)[11]
  - ISO/IEC 27000-Reihe[12]
  - IT-Grundschutz[13]
- **Best Practices**
  - OWASP (Open Web Application Security Project)[14], z. B. SAMM (Software Assurance Maturity Model)[15]

[11] https://commoncriteriaportal.org/, aufgerufen am 18. April 2023
[12] https://www.iso.org/isoiec-27001-information-security.html, aufgerufen am 18. April 2023
[13] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html, aufgerufen am 18. April 2023
[14] https://www.owasp.org/, aufgerufen am 18. April 2023
[15] https://owaspsamm.org/, aufgerufen am 18. April 2023

Entwicklung und Veröffentlichung

- **Entwickler und Herausgeber** von Standards sind typischerweise nationale oder internationale, staatliche oder unabhängige Organisationen, z. B. :
  - Joint Technical Committee 1 „Information Security“ (**JTC 1**) wird aus International Organization for Standardization (**ISO**) und International Electrotechnical Commission (**IEC**) gebildet und ist international für Bereich IT-Sicherheit zuständig.
  - Innerhalb von JTC 1 ist das Subcommittee 27 „IT security techniques“ zuständig, welches in Working groups, z. B. „WG 2 Cryptography and security mechanisms“, organisiert ist.
- Best Practices sind hingegen typischweise durch eine Interessensgemeinschaft entwickelt, häufig getrieben durch Unternehmen.

Stand der Technik

- Mittels Standardisierung wird ein **Stand der Technik** definiert (mit juristischer Bedeutung).
- Die Einhaltung von Standards und Best Practices wird typischerweise bestimmt durch
  - Gesetze, z. B. Datenschutz-Grundverordnung (**DS-GVO**)[16]
  - Regulatorische, oft branchenspezifische Anforderungen, z. B. Payment Card Industry Data Security Standard (**PCI-DSS**)[17]
  - Nationale, staatliche Organisationen, z. B. Institute of Electrical and Electronics Engineers (**IEEE**) und National Institute of Standards and Technology (**NIST**)

[16] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32016R0679, aufgerufen am 18. April 2023

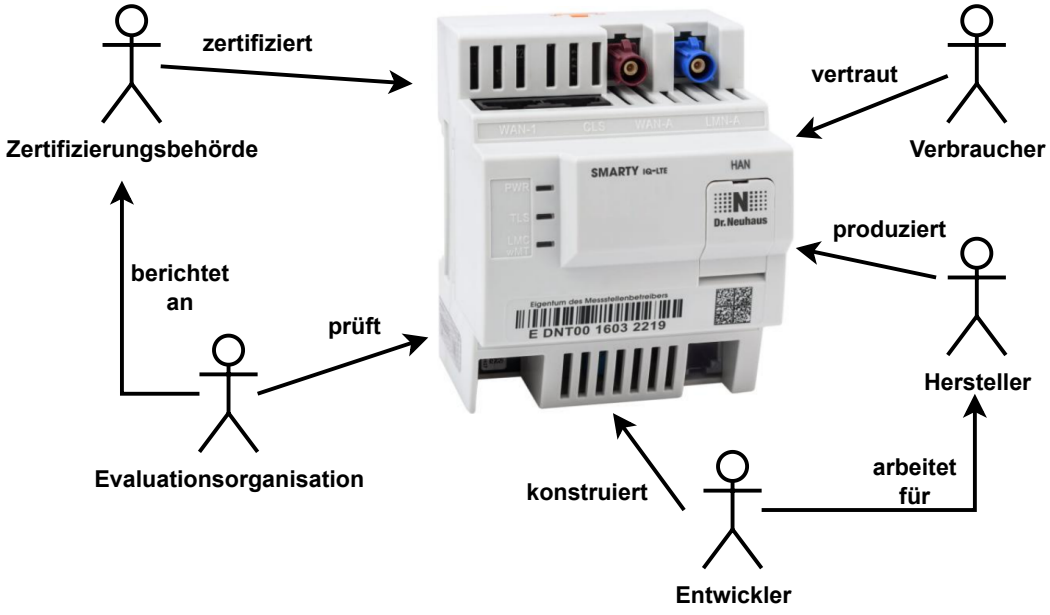
[17] https://docs-prv.pcisecuritystandards.org/Software%20Security/Standard/PCI-Secure-Software-Standard-v1_2.pdf, aufgerufen am 18. April 2023

Common Criteria

- **Produktzertifizierung**
- Formale Basis: **Common Criteria Recognition Arrangement (CCRA)**
- Technische Basis:
  - Common Criteria for Information Technology Security Evaluation (CC, 2022a, 2022b, 2022c, 2022d, 2022e)
  - Common Methodology for Information Technology Security Evaluation (CEM, 2022)
- Aktuelle Version 2022 Release 1 entspricht ISO/IEC 15408:2022 und ISO/IEC 18045:2022.
- http://www.commoncriteriaportal.org/, aufgerufen am 18. April 2023
- **Praxisrelevanz**: Software, Hardware, Hochrisikofelder (z. B. Regierung, Gesundheitswesen, Bank, Versicherung)

Entwicklungs- , Evaluations- und Zertifizierungsgeschäft

Fachhochschule Dortmund
University of Applied Sciences and Arts



IT-Sicherheitsqualitätskontrolle durch Entwickler / Evaluatoren

Fachhochschule Dortmund
University of Applied Sciences and Arts

Assurance class	Assurance family	Assurance components by evaluation assurance level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life-cycle support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
ST evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Table 1 aus CC Part 5 (siehe oben)

- **IT-Sicherheitsqualitäts-kontrolle** angewandt
  - während Entwicklung
  - wiederholt und ergänzt während Evaluation
- Getrieben durch **Entwicklungsartefakte**
- Verbrauchersicht: Je höher die EAL, umso mehr **Vertrauen** in das Produkt.
- Beispiel:
  - Security Target für SMARTY IQ-SMGW LTE von Sagemcom Dr. Neuhaus GmbH[18]
  - **Evaluation Assurance Level (EAL) 4** ergänzt um AVA_VAN.5 und ALC_FLR.2

[18] https://commoncriteriaportal.org/files/epfiles/0822V3b_pdf.pdf, zuletzt aufgerufen am 18. April 2023

Entwicklungs- und Evaluationsanforderungen

- Grundsätzlich wenden Entwicklung und Evaluation **ähnliche IT-Sicherheitsqualitätskontrolle** an
- Basierend auf **Angreifermodell** und EAL
- Abdeckung des **gesamten Produktlebenszyklus** (Entwicklung, Produktion, Betrieb, Wartung)
- Common Criteria fordert z. B.:
  - **Konsistenz- und Vollständigkeitsprüfungen**
  - **Site audits** (Build, Deployment, Incident Management)
  - **Schwachstellenanalyse** (insb. Code Review und Penetrationstests)
  - **Formale Verifikation** (Model Checking, Theorem Proving)

Common Criteria
Bedrohungsanalyse

Bedrohungsanalyse

- **CC Herstelleraufgabe** (CC, 2022a, Kapitel 7.1)
- Definition von **Sicherheitsproblemen** bestehend aus
  - **Bedrohungen**
  - **Organisatorische Sicherheitsrichtlinien**
  - **Annahmen**

Bedrohungen

- Eine **Bedrohung** (CC, 2022a, Kapitel 7.1.2) besteht aus einer
  - **böswilligen Aktion (adverse action)** *durchgeführt von einem*
  - **böswillig Handelndem (threat agent)** *abzielend auf eine*
  - **schützenswerte Ressource (asset)** bzw. den zugehörigen Schutzzielen.
- Betrachten das ungeschützte System (im Gegensatz zu Schwachstellen): „Was kann passieren, wenn das TOE nicht vorhanden ist?“
- Adressiert durch TOE, Umgebung oder Kombination aus beidem
- Optional, wenn mindestens eine organisatorische Sicherheitsrichtlinie definiert wurde

Identifikation und Spezifikation von Bedrohungen

- Assets sind **physikalische oder logische Teile der Betriebsumgebung** des TOE, z. B. Computerraum, LAN mit Internetanbindung
  - Welche Assets sind für potentielle Käufer des TOE so wertvoll, dass diese das TOE zum Schutz der Assets tatsächlich kaufen?
- Adverse actions **beeinflussen Eigenschaften von Assets** derart, dass es zu **Wertverlusten** kommt, z. B. abhören innerhalb eines LAN
  - Warum sind Assets wertvoll und wie könnten Wertverluste herbeigeführt werden?
- Threat agents sind **Individuen oder Typen** (im Sinne von Mengen gleichartiger Individuen, z. B. Organisationen), z. B. Hacker, Benutzer
  - Wer oder was hat ein Interesse daran Wertverluste für Assets herbeizuführen?

Organisatorische Sicherheitsrichtlinien

- **Organisatorische Sicherheitsrichtlinien** (CC, 2022a, Kapitel 7.1.3)
- Häufig abgeleitet aus **rechtlichen und regulatorischen Rahmenbedingungen** sowie **Informationssicherheitsmanagementsystemen (ISMS)**
- z. B. Richtlinie 1999/93/EG „Rahmenbedingungen für elektronische Signaturen“: „…Sichere Signaturerstellungseinheiten müssen durch geeignete Technik und Verfahren zumindest gewährleisten, daß a) die für die Erzeugung der Signatur verwendeten Signaturerstellungsdaten praktisch nur einmal auftreten können und daß ihre Geheimhaltung hinreichend gewährleistet ist …“[19]
- Optional, wenn mindestens eine Bedrohung definiert wurde

[19] https://eur-lex.europa.eu/eli/dir/1999/93/oj, aufgerufen am 18. April 2023

Annahmen

- **Annahmen** (CC, 2022a, Kapitel 7.1.4)
- Optional
- **Aussagen** über die Betriebsumgebung, die einen **probabilistischen Charakter** haben (und damit keine Fakten sind)
- Annahmen müssen „realistisch“ sein, d. h. es ist bereits bekannt, dass die Aussagen gelten oder die Aussagen lassen sich tatsächlich praktisch umsetzen.
- z. B. der Zugriff auf die physikalische Betriebsumgebung des TOE ist abgesichert, da sich das TOE in einem abschließbaren Raum befindet. (Entsprechend müssen Bedrohungen durch physikalische Angriffe nicht betrachtet werden.)

Weitere Herstelleraufgaben im Rahmen des Security Targets

- Basierend auf den Sicherheitsproblemen werden **Sicherheitsziele** (CC, 2022a, Kapitel 7.2) abgeleitet, welche implementierungsunabhängige Lösungen für die jeweiligen Sicherheitsprobleme natürlichsprachlich beschreiben.
- **Sicherheitsanforderungen** (CC, 2022a, Kapitel 7.3.2) operationalisieren Sicherheitsziele soweit, dass eine konkrete Implementierung vorgenommen werden kann. Die CC bietet einen Katalog von Mustern für häufig auftretende Sicherheitsanforderungen (CC, 2022b).
- **Prüfanforderungen** (CC, 2022a, Kapitel 7.3.3) beschreiben wie ein TOE geprüft werden muss abhängig von der Prüftiefe. Die CC bietet einen Katalog von standardisierten Prüfanforderungen (CC, 2022c).

Common Criteria
Schwachstellenanalyse

Schwachstellenanalyse I

- **CC Prüfaufgabe** (CEM, 2022, Kapitel 17.2 und Anhang B)
- **Entwicklung** und **Betrieb**
- **Existenz** und **Ausnutzbarkeit** von Schwachstellen
  - **Identifikation**, z. B. mithilfe Code Review, Code Analyse, Fuzzy Testing
  - **Beurteilung** hinsichtlich Angreifermodell
  - **Validierung**, z. B. mithilfe von Penetrationstests

Schwachstellenanalyse II

- **Kategorisierung** von Schwachstellen:
  - Umgehung von Sicherheitsmaßnahmen
  - Unerlaubte Veränderung und Beeinflussung
  - Direkte Angriffe
  - Überwachung
  - Missbrauch

Angreifermodell

- **Angreifermodell** (Angriffspotential) als Funktion aus
  - Benötigter Zeit zur Identifikation und Ausnutzung
  - Fähigkeiten
  - Wissen über das Ziel
  - Zur Verfügung stehender Zeit zur Identifikation und Ausnutzung
  - Ausstattung

Faktoren für Angreifermodell I

Factor	Value
Elapsed Time	
<= one day	0
<= one week	1
<= two weeks	2
<= one month	4
<= two months	7
<= three months	10
<= four months	13
<= five months	15
<= six months	17
> six months	19
Expertise	
Layman	0
Proficient	3[a]
Expert	6
Multiple experts	8

Tabelle B.2 aus CEM, 2022

Faktoren für Angreifermodell II

Knowledge of TOE	
Public	0
Restricted	3
Sensitive	7
Critical	11
Window of Opportunity	
Unnecessary / unlimited access	0
Easy	1
Moderate	4
Difficult	10
None	**[b]
Equipment	
Standard	0
Specialised	4[c]
Bespoke	7
Multiple bespoke	9

Tabelle B.2 aus CEM, 2022

Schwachstellenbewertung

Values	Attack potential required to exploit scenario:	Meets assurance components:	Failure of components:
0-9	Basic	-	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4, AVA_VAN.5
10-13	Enhanced-Basic	AVA_VAN.1, AVA_VAN.2	AVA_VAN.3, AVA_VAN.4, AVA_VAN.5
14-19	Moderate	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3	AVA_VAN.4, AVA_VAN.5
20-24	High	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4	AVA_VAN.5
=>25	Beyond High	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4, AVA_VAN.5	-

Tabelle B.3 aus CEM, 2022

Beispiel Schwachstellenanalyse

- System Bus Radio[20] als direkter Angriff im Betrieb
- Beurteilung hinsichtlich Angreifermodell:

  Zeit weniger als ein Tag (*value* = 0), Identifikation über TOE Wissen und Ausnutzung einfach, da Exploit vorhanden

  Expertise Laie (*value* = 0), da Exploit vorhanden

  Wissen über das TOE eingeschränkt (*value* = 3), da nur auf bestimmten Rechnern ausführbar

  Ausrüstung Standard (*value* = 0), da PC ausreicht

  Gesamtergebnis *value* = 3, Summe der Einzelergebnisse

- Entsprechend reicht bereits ein Angriffspotential der Kategorie „basic“ aus.

Wie könnte man dem Sicherheitsproblem begegnen?

[20] https://fulldecent.github.io/system-bus-radio/, aufgerufen am 18. April 2023

Zusammenfassung

Zusammenfassung

- Verankerung der Informationssicherheit im deutschen Recht definiert
- Grundlagen der europäischen Datenschutz-Grundverordnung eingeführt
- Bedeutung von Standards und Best Practices für die Informationssicherheit kennengelernt
- Common Criteria, insbesondere Bedrohungs- und Schwachstellenanalyse, vertieft

Weiterführende Literatur

Weiterführende Literatur

- *IT-Sicherheit – Konzepte - Verfahren - Protokolle*, Kapitel 1.3.3 von Eckert (2023)
- *Handbuch Datenschutz und IT-Sicherheit* von Schläger und Thode (2022)

Literatur I

CC. (2022a). Common Criteria Part 1: Introduction and general model. https://www.commoncriteriaportal.org/files/ccfiles/CC2022PART1R1.pdf (siehe S. 23, 28, 29, 31–33).

CC. (2022b). Common Criteria Part 2: Security functional requirements. https://www.commoncriteriaportal.org/files/ccfiles/CC2022PART2R1.pdf (siehe S. 23, 33).

CC. (2022c). Common Criteria Part 3: Security assurance requirements. https://www.commoncriteriaportal.org/files/ccfiles/CC2022PART3R1.pdf (siehe S. 23, 33).

CC. (2022d). Common Criteria Part 4: Pre-defined packages of security requirements. https://www.commoncriteriaportal.org/files/ccfiles/CC2022PART5R1.pdf (siehe S. 23).

Literatur II

CC. (2022e). Common Criteria Part 5: Framework for the specification of evaluation methods and activities. https://www.commoncriteriaportal.org/files/ccfiles/CC2022PART4R1.pdf (siehe S. 23).

CEM. (2022). Common Methodology for Information Technology Security Evaluation [Release 1]. https://www.commoncriteriaportal.org/files/ccfiles/CEM2022R1.pdf (siehe S. 23, 35, 38–40).

Eckert, C. (2023). *IT-Sicherheit: Konzepte - Verfahren - Protokolle* (11. Aufl.). De Gruyter Oldenbourg. (Siehe S. 45).

Reinhard, T., Pohl, L., & Capellaro, H.-C. (2007). *IT-Sicherheit und Recht: Rechtliche und technisch-organisatorische Aspekte für Unternehmen*. Erich Schmidt Verlag. (Siehe S. 9).

Schläger, U., & Thode, J.-C. (2022). *Handbuch Datenschutz und IT-Sicherheit* (2. Aufl.). Erich Schmidt Verlag GmbH & Co. KG Berlin. (Siehe S. 45).