



Hochschule Neubrandenburg  
University of Applied Sciences

Dr. Andreas Müller

# **Modul:**

## **Datenschutz und betriebliche IT-Sicherheit**

Studienbrief

### **Master-Studiengang:**

## **Digitalisierung und Sozialstrukturwandel**

Stand: Sommersemester 2018

GEFÖRDERT VOM



Bundesministerium  
für Bildung  
und Forschung

# Inhaltsverzeichnis

<b>Abbildungsverzeichnis</b> .....	<b>V</b>
<b>Tabellenverzeichnis</b> .....	<b>VI</b>
<b>Abkürzungsverzeichnis</b> .....	<b>VII</b>
<b>Einleitung</b> .....	<b>1</b>
<b>Kapitel 1</b> .....	<b>2</b>
<b>1 Einführung</b> .....	<b>2</b>
1.1 Grundlegende Betrachtung .....	2
1.2 Spannungsfeld Datenschutz und Ethik.....	3
1.3 Lernkontrollaufgaben .....	5
<b>Kapitel 2</b> .....	<b>6</b>
<b>2 Datenschutz</b> .....	<b>6</b>
2.1 Lernziele .....	6
2.2 Definitionen, Grundbegriffe .....	6
2.3 Ziele des Datenschutzes .....	7
2.3.1 Prinzip der Rechtmäßigkeit der Erhebung (und Verarbeitung).....	7
2.3.2 Prinzip der Richtigkeit.....	8
2.3.3 Prinzip der Zweckgebundenheit .....	8
2.3.4 Prinzip der Verhältnismäßigkeit.....	8
2.3.5 Prinzip der Transparenz .....	9
2.3.6 Prinzip des garantierten Zugriffs des Betroffenen.....	10
2.3.7 Prinzip der Sicherheit .....	10
2.3.8 Prinzip der Haftung.....	10
2.4 Rechte und Pflichten im Datenschutz.....	10
2.4.1 Auskunftsrecht .....	11
2.4.2 Berichtigung fehlerhafter oder unvollständiger Daten .....	11
2.4.3 Benachrichtigung über eine Datenerhebung.....	11
2.4.4 Löschung .....	11
2.4.5 Sperrung .....	11
2.4.6 Schadensersatz .....	11
2.5 Maßnahmen zum Datenschutz.....	12
2.5.1 Organisatorische Maßnahmen .....	12
2.5.2 Technische Maßnahmen .....	13
2.6 Exkurs Rechtliche Grundlagen .....	14
2.6.1 Bundesdatenschutzgesetz .....	14
2.6.2 EU-Datenschutzgrundverordnung .....	16
2.6.3 Weitere relevante Datenschutzvorschriften .....	18
2.7 Datenschutzbeauftragter .....	19

2.8	Zusammenfassung.....	21
2.9	Lernkontrollaufgaben .....	21
<b>Kapitel 3</b>	.....	<b>22</b>
<b>3</b>	<b>Datensicherheit</b> .....	<b>22</b>
3.1	Lernziele .....	22
3.2	Definitionen, Grundbegriffe .....	22
3.3	Ziele der Datensicherheit .....	22
3.3.1	Datenintegrität.....	22
3.3.2	Authentizität .....	23
3.3.3	Vertraulichkeit .....	23
3.3.4	Verfügbarkeit.....	23
3.3.5	Verbindlichkeit.....	23
3.4	Rechnersicherheit .....	23
3.5	Kommunikationssicherheit .....	24
3.5.1	Integrität .....	24
3.5.2	Vertraulichkeit .....	25
3.5.3	Verfügbarkeit.....	25
3.5.4	Authentizität .....	26
3.6	Maßnahmen zur Datensicherheit .....	27
3.6.1	Zutrittskontrolle.....	27
3.6.2	Eingabekontrolle .....	27
3.6.3	Zugangskontrolle.....	27
3.6.4	Zugriffskontrolle.....	27
3.6.5	Kontrolle der Weiterleitung .....	28
3.6.6	Kontrolle der Verfügbarkeit.....	28
3.6.7	Kontrolle der separaten Haltung von Daten.....	28
3.7	Widersprüche bzw. Abwägungen .....	29
3.8	Zusammenfassung.....	29
3.9	Lernkontrollaufgaben .....	29
<b>Kapitel 4</b>	.....	<b>30</b>
<b>4</b>	<b>IT-Sicherheit</b> .....	<b>30</b>
4.1	Lernziele .....	30
4.2	Definitionen, Grundbegriffe .....	30
4.2.1	Safety.....	30
4.2.2	Security .....	31
4.3	Mögliche Bedrohungsszenarien .....	32
4.3.1	Aktive Angriffe .....	32
4.3.2	Passive Angriffe .....	34
4.3.3	System- oder Bedienungsfehler .....	34

4.4	Verschlüsselung.....	34
4.4.1	Symmetrische Verschlüsselung.....	35
4.4.2	Asymmetrische Verschlüsselung.....	35
4.4.3	Hybride Verschlüsselung.....	36
4.5	Viren, Trojaner und Co. ....	37
4.5.1	Computervirus.....	37
4.5.2	Computerwürmer .....	38
4.5.3	Trojaner.....	39
4.5.4	Spyware .....	40
4.6	Schutzmaßnahmen .....	40
4.6.1	Antivirenprogramme .....	40
4.6.2	Firewall.....	42
	Destop-Firewall .....	42
	Hardware-Firewall .....	43
	Verfahrensweise .....	43
4.6.3	Proxy-Server .....	44
4.7	Zusammenfassung.....	44
4.8	Lernkontrollaufgaben .....	45
	<b>Kapitel 5.....</b>	<b>46</b>
	<b>5 Lösungswege und Handlungsanleitungen.....</b>	<b>46</b>
5.1	Lernziele .....	46
5.2	Checkliste zu organisatorischen und technischen Maßnahmen .....	46
5.2.1	Die Organisationskontrolle .....	46
5.2.2	Die Zutrittskontrolle .....	48
5.2.3	Die Zugangskontrolle .....	50
5.2.4	Die Zugriffskontrolle .....	52
5.2.5	Die Weitergabekontrolle .....	54
5.2.6	Die Eingabekontrolle .....	56
5.2.7	Die Auftragskontrolle .....	56
5.2.8	Die Verfügbarkeitskontrolle .....	57
5.2.9	Die Trennungskontrolle .....	59
5.2.10	Kontrolle des Internetauftrittes.....	60
5.2.11	Kontrolle des internen WLAN-Netzes .....	61
5.3	Zusammenfassung.....	62
5.4	Lernkontrollaufgaben .....	62
	<b>Kapitel 6.....</b>	<b>63</b>
	<b>6 Anwendungsfälle – 2 Fallbeispiele .....</b>	<b>63</b>
6.1	Lernziele .....	63
6.2	Digitalisierung medizinischer Dienstleister.....	63
6.2.1	Der Hausarzt.....	63

6.2.2 Die Dienstleister .....	64
6.2.3 Die Patienten.....	64
6.3 Sanddornmarmelade oder wie die Globalisierung sicher gelingt .....	65
6.3.1 Das Unternehmen .....	65
6.3.2 Die Kunden .....	65
6.3.3 Partner und Lieferanten.....	66
6.4 Lernkontrollaufgaben .....	66
<b>Schlussbetrachtung .....</b>	<b>67</b>
<b>Literaturverzeichnis .....</b>	<b>68</b>

## Abbildungsverzeichnis

Abbildung 1:	Rechte-Rollen-Matrix.....	13
Abbildung 2:	Beispiel einer Rechte-Rollen-Matrix in einem MS-Windows-System.....	14
Abbildung 3:	Verletzung der Datenintegrität .....	24
Abbildung 4:	Angriff auf die Vertraulichkeit.....	25
Abbildung 5:	Beeinträchtigung der Datenverfügbarkeit.....	26
Abbildung 6:	Verletzung der Authentizität.....	26
Abbildung 7:	Mögliche Bedrohungsszenarien.....	32
Abbildung 8:	Beispiel einer DoS-Attacke .....	33
Abbildung 9:	Verfahrensweise symmetrische Verschlüsselung .....	35
Abbildung 10:	Verfahrensweise asymmetrische Verschlüsselung .....	36
Abbildung 11:	Prinzip einer Firewall .....	42
Abbildung 12:	Firewall - DMZ .....	44

## Tabellenverzeichnis

Tabelle 1:	Organisationskontrolle.....	48
Tabelle 2:	Zutrittskontrolle.....	49
Tabelle 3:	Zugangskontrolle.....	52
Tabelle 4:	Zugriffskontrolle.....	54
Tabelle 5:	Weitergabekontrolle .....	55
Tabelle 6:	Eingabekontrolle .....	56
Tabelle 7:	Auftragskontrolle .....	57
Tabelle 8:	Verfügbarkeitskontrolle.....	59
Tabelle 9:	Trennungskontrolle.....	60
Tabelle 10:	Kontrolle des Internetauftritts.....	61
Tabelle 11:	Kontrolle WLAN.....	62

## Abkürzungsverzeichnis

AAL	Ambient Assisted Living
AES	Advanced Encryption Standard
AVD	Auftragsdatenverarbeitung
BDSB	Bundesdatenschutzbeauftragter
BDSG	Bundesdatenschutzgesetz
BMBF	Bundesministerium für Bildung und Forschung
DES	Data Encryption Standard
DEÜV	Datenerfassungs- und übermittlungsverordnung
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarisierte Zone (Firewall)
DoS	Denial of Service
DSB	Datenschutzbeauftragter
DSGVO	Datenschutzgrundverordnung
DT	Datenträger
DV	Datenverarbeitung
EU	Europäische Union
FTP	File Transfer Protocol
HS-NB	Hochschule Neubrandenburg
HTTP	Hypertext Transfer Protocol
HTTP/S	Hypertext Transfer Protocol Secure
IDEA	International Data Encryption Algorithm
IP	Internetprotokoll
IT	Informationstechnologie
IuK	Informations- und Kommunikationstechnologie
LAN	Local Area Network
MAC	Media Access Control
P2P	Peer-to-Peer
PC	Personal Computer
PGP	Pretty Good Privacy
PIN	Personal Identification Number
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SSID	Service Set Identifier
SSH	Secure Shell
SSL/TLS	Secure Sockets Layer / Transport Layer Security
TK	Telekommunikation
TMG	Telemediengesetz
USB	Universal Serial Bus
USV	unterbrechungsfreie Stromversorgung
WLAN	Wireless Local Area Network



## Einleitung

Die Digitalisierung bestimmt immer deutlicher immer breitere Bereiche des beruflichen und privaten Lebens. Überall werden Daten erhoben, weitergeleitet, verändert, gespeichert und abgerufen.

In diesem Studienbrief werden die Grundbegriffe des Datenschutzes und der Datensicherheit für Anwender aus primär nichttechnischen Berufen erläutert. Das Ziel dieses Kurses ist es, in einem berufsbegleitenden Studium grundlegende Kenntnisse in den Bereichen des betrieblichen Datenschutzes und der Datensicherheit zu vermitteln. Insbesondere im Zuge einer umfänglichen Digitalisierung auch in nichttechnischen Berufsbildern werden diese Kenntnisse in vielfältigen Arbeits- und Lebensbereichen immer wichtiger. Diesen Herausforderungen soll in diesem Kurs begegnet und eine Basis für eine zukunftsorientierte berufliche Perspektive gelegt werden.

Neben den technischen werden überdies die rechtlichen und organisatorischen Aspekte beleuchtet.