



# Inhaltsverzeichnis

<b>AUTORENTTEAM .....</b>	III
<b>EINLEITUNG.....</b>	v
<b>SEMINARZIELE .....</b>	vi
<b>INHALTSVERZEICHNIS.....</b>	vii
<b>1. Das Internet.....</b>	1
1.1. Die Funktionsweise des Internet.....	1
1.2. Zugang zum Internet.....	1
1.3. Internetdienste .....	2
1.4. Der Browser .....	2
1.5. Der Webserver .....	3
1.6. Aktive Inhalte.....	4
1.7. Java Applets.....	4
1.8. JavaScript / JScript .....	5
1.9. ActiveX-Controls .....	5
1.10. VBScript / VB.NET .....	6
1.11. Adobe Flash & Co. ....	6
1.12. Cookies .....	7
1.13. SSL, TLS und https .....	8
Notizen .....	8
<b>2. Web 2.0, Social Community oder „Das Mitmachweb“ .....</b>	9
2.1. Soziale Netzwerke .....	9
Notizen .....	12
<b>3. Bedrohung, Angriffe und Gefahren aus dem Internet.....</b>	13
3.1. Einführung .....	13
3.2. Computerviren und andere Schädlinge .....	14
3.3. Tarnmechanismen .....	14
3.4. Infizierung und Verbreitung .....	15
3.5. Virenarten.....	16
3.5.1 Datei- und Linkviren .....	16
3.5.2 Makroviren .....	16
3.5.3 Skriptviren .....	17
3.5.4 Bootsektorviren .....	17
3.5.5 Hybridviren .....	17
3.5.6 Dropper .....	17
3.6. Andere Schädlingsarten.....	18
3.6.1 Würmer.....	18
3.6.2 Trojanische Pferde .....	18
3.6.3 Rootkits .....	19
3.6.4 Backdoor .....	19
3.6.5 Keylogger .....	19
3.6.6 Crimeware .....	20
3.6.7 Scareware / Rogueware / Ransomware .....	20
3.6.8 Spy- / Adware.....	21



3.6.9	Riskware .....	21
3.7.	Angriffsmethoden .....	22
3.7.1	Spoofing .....	22
3.7.2	Sniffing.....	22
3.7.3	Botnet .....	23
3.7.4	Denial-of-Service – DoS .....	23
3.7.5	Man-in-the-middle-Attacke .....	23
3.7.6	Brute-Force / Wörterbuchattacke .....	23
3.8.	Soziale Angriffsmethoden .....	24
3.8.1	Gefahr Mensch und die Sensibilisierung der Mitarbeiter .....	24
3.8.2	Gefahren durch private Mails .....	25
3.8.3	Hoaxes .....	26
3.8.4	Gefahr durch Instant Messaging .....	26
3.8.5	Social Engineering.....	28
3.8.6	Dumpster Diving .....	28
3.8.7	Social Engineering über das Telefon .....	29
3.8.8	Vishing .....	29
3.8.9	Social Engineering über das Internet .....	29
3.8.10	Social-Engineering durch Phishing .....	30
3.8.11	Reverse Social Engineering .....	30
	Notizen .....	31
<b>4.</b>	<b>Schutz vor Gefahren aus dem Internet .....</b>	<b>33</b>
4.1.	Update des Betriebssystems.....	33
4.2.	Browserupdate .....	33
4.3.	Browsereinstellungen .....	33
4.4.	Aufmerksamkeit beim Surfen und Arbeiten.....	34
4.5.	Sicherheitsstatus überprüfen.....	34
4.6.	Passwort.....	37
4.6.1	Nutzen Sie ein System für verschiedene Passwörter .....	37
4.6.2	Passwort Generator und Prüfer.....	37
4.7.	Umgang mit Passwörtern .....	39
4.8.	Netzwerk.....	40
4.9.	Firewall .....	40
4.10.	VirensScanner .....	43
4.11.	MalwaresScanner .....	43
4.12.	Nützliche Tools und Vorgehensweisen .....	44
4.12.1	Andere Updates.....	44
4.12.2	Browsertools.....	44
	NoScript .....	44
	BetterPrivacy .....	44
	privacyfix.....	45
4.12.3	Suche nach laufenden Prozessen.....	45
4.13.	Verschlüsselung .....	45
	Notizen .....	46
<b>5.</b>	<b>Updates und Einstellungen des Webbrowsers .....</b>	<b>47</b>
5.1.	Vorbereitungen .....	47
5.1.1	Windows Update .....	47
5.1.2	Update des Internet Explorers.....	49
5.1.3	Update von Mozilla Firefox .....	50
5.2.	Einstellungen im Internet Explorer .....	52
5.2.1	Allgemeine Einstellungen .....	52



5.2.2	Das Zonenkonzept des Internet-Explorer .....	54
5.2.3	Datenschutz .....	57
5.2.4	Inhalte.....	60
5.2.5	Programme .....	63
5.2.6	Erweiterte Browzereinstellungen .....	64
5.2.7	Zusätzliche Sicherheitsfunktionen .....	65
	InPrivate-Browsen.....	66
	Tracking-Schutz .....	66
	ActiveX-Filterung .....	68
	SmartScreen-Filter .....	69
5.3.	Einstellungen bei Mozilla Firefox .....	71
5.3.1	Allgemeine Einstellungen.....	71
5.3.2	Tabs .....	72
5.3.3	Inhalt.....	73
5.3.4	Anwendungen .....	74
5.3.5	Datenschutz .....	75
5.3.6	Sicherheit .....	80
5.3.7	Sync .....	82
5.3.8	Erweitert .....	82
	Allgemein .....	82
	Datenübermittlung .....	83
	Netzwerk .....	84
	Updates .....	85
	Zertifikate .....	87
5.3.9	Add-Ons-Manager.....	88
	Notizen .....	93
<b>6.</b>	<b>Voice Over IP (VoIP).....</b>	<b>94</b>
6.1.	Funktionsprinzip .....	94
6.2.	Sicherheitsaspekte .....	95
	Notizen .....	96
<b>7.</b>	<b>BYOD - Bring Your Own Device.....</b>	<b>97</b>
7.1.	Einleitung – Vor- und Nachteile von BYOD .....	97
7.2.	Sicherheit bei BYOD .....	98
7.3.	Jailbreak / Root .....	99
7.4.	Mobile Device Management .....	99
	Notizen .....	100
<b>8.</b>	<b>Cloud-Computing .....</b>	<b>101</b>
8.1.	Einführung .....	101
8.2.	Sicherheitsaspekte und Risiken von Cloud-Computing.....	103
	Standort.....	103
	Verschlüsselung .....	103
	Weitere Aspekte.....	103
<b>9.</b>	<b>Datenschutz .....</b>	<b>104</b>
9.1.	Was versteht man unter Datenschutz?.....	104
9.2.	Rechte der Betroffenen .....	105
9.3.	Anforderungen an den Datenschutz .....	105
9.3.1	Grundforderung auf Vertraulichkeit.....	105
9.3.2	Grundforderung auf Datenintegrität .....	106

9.3.3	Grundforderung auf Verfügbarkeit.....	106
9.4.	Zielsetzung des Datenschutzes .....	107
9.5.	Berichtigung, Sperrung, Löschung von Daten und Widerspruchsrecht .....	107
9.5.1	Berichtigung.....	107
9.5.2	Löschen .....	107
9.5.3	Widerspruchsrecht.....	108
9.5.4	Unterlassung und Beseitigung .....	108
9.5.5	Wahrung des Datengeheimnisses .....	108
9.6.	Rechtsvorschriften des Datenschutzes .....	108
9.6.1	Anwendungsbereich der LDSG .....	108
9.7.	Datenschutz und Datensicherheit in Ausbildungsstätten.....	109
9.7.1	Übergreifende Grundsätze und Verfahren zur Datensicherung beim Einsatz von Datenverarbeitungssystemen einschl. Internet, E-Mail und Kommunikations-Diensten .....	109
9.7.2	Generelle Einschränkungen für die automatisierte Verarbeitung personenbezogener Daten.....	110
9.7.3	Einsatz von tragbaren Computern.....	110
9.7.4	Einsatz privater Computer für die Bearbeitung personenbezogener Daten zu Ausbildungszwecken .....	111
9.7.5	Versendung von beweglichen Datenträgern .....	111
9.7.6	Nutzung von Internet- und Maildiensten, Telefaxgeräten .....	111
9.7.7	Technische Aspekte .....	112
9.7.8	Rechtliche Aspekte.....	112
9.7.9	Urheberrechtsgesetz und Kunst-Urhebergesetz .....	113
9.7.10	Private Nutzung des Internets .....	113
9.8.	Orientierungshilfe für die Videoüberwachung an und in Ausbildungsstätten .....	114
9.8.1	Grundsätze .....	114
9.8.2	Videoüberwachung in öffentlich zugänglichen Bereichen der Ausbildungsstätten .....	114
9.8.3	Videoüberwachung in nicht öffentlich zugänglichen Bereichen der Ausbildungsstätten .....	115
9.8.4	Hinweispflicht.....	115
9.8.5	Kamera-Attrappen .....	115
9.8.6	Die Behandlung aufgezeichneter Videodaten .....	115
9.8.7	Dienstanweisung .....	116
9.8.8	Sonstige institutionelle Beteiligungen.....	116
9.8.9	Evaluation .....	117
	Notizen .....	117
	<b>Literaturverzeichnis.....</b>	<b>118</b>
	<b>Abbildungsverzeichnis.....</b>	<b>119</b>
	<b>Stichwortverzeichnis .....</b>	<b>121</b>