INHALT

1 BEGRIFFE ZUR SICHERHEIT VON DATEN 7

1.1 Datenbedrohung 7

1.1.1 Unterschied zwischen Informationen und Daten 7

1.1.2 Cybercrime, Hacker 8

1.1.3 Bedrohung für Daten 10

1.1.4 Datenbedrohung durch höhere Gewalt 11

1.1.5 Bedrohung für Daten im Cloud-Computing: Datenkontrolle, möglicher Verlust der Privatsphäre 12

1.2 Wert von Informationen 13

1.2.1 Merkmale von Datensicherheit 14

1.2.2 Wahrheitswert der Daten – Fake-News 15

1.2.3 Personenbezogene Daten schützen 16

1.2.4 Firmendaten schützen 17

1.2.5 Grundsätze für Schutz von Daten und der Privatsphäre 17

1.2.6 Wer sind Betroffener, Auftraggeber oder Verantwortlicher 20

1.2.7 Grundsätze und Richtlinien 21

1.3 Persönliche Sicherheit 22

1.3.1 Was versteht man unter Social Engineering 22

1.3.2 Methoden des Social Engineering 22

1.3.3 Identitätsdiebstahl, Identitätsmissbrauch 24

1.3.4 Wie erfolgt ein Identitätsdiebstahls 25

1.4 Sicherheit für Dateien 26

1.4.1 Makro-Sicherheitseinstellungen 26

1.4.2 Verschlüsselung und Passwortnutzung 27

1.4.3 Dateien, Ordner oder Laufwerk verschlüsseln 28

1.4.4 Dateien mit Passwort schützen 34

2 MALWARE 37

2.1 Arten und Funktionsweisen 37

2.1.1 Malware erkennen 37

2.1.2 Selbst verbreitende Malware 38

2.1.3 Arten von Malware 39

2.2 Schutz 41
2.2.1 Funktionsweise von Antiviren-Software 42
2.2.2 Antiviren-Software auf Computer installieren 42
2.2.3 Regelmäßige Software-Updates 43
2.2.4 Laufwerke, Ordner und Dateien mit Antiviren-Software scannen 44
2.2.5 Risiko bei veralteter und nicht mehr unterstützter Software 45

2.3 Problemlösung und -behebung 45
2.3.1 Quarantäne und die Auswirkung auf infizierte oder verdächtige Dateien 45
2.3.2 Umgang mit infizierten oder verdächtigen Dateien 46
2.3.3 Malware-Angriff mithilfe von Online-Ressourcen identifizieren 46

Wissens-Check 47

3 SICHERHEIT IM NETZWERK 49

3.1 Netzwerke und Verbindungen 49
3.1.1 Netzwerktypen 49
3.1.2 Sicherheitsrisiko bei Verbindung zu einem Netzwerk 50
3.1.3 Aufgaben der Netzwerk-Administration 50
3.1.4 Funktion und Grenzen einer Firewall 51
3.1.5 Personal Firewall ein- und ausschalten 52

3.2 Sicherheit im drahtlosen Netz 54
3.2.1 WEP, WPA, WPA2, MAC-Filter und SSID 54
3.2.2 Welche Gefahren drohen bei ungeschützten Netzwerken 57
3.2.3 Persönlicher Hotspot 58
3.2.4 Persönlichen Hotspot ein- und ausschalten 59

Wissens-Check 60

4 ZUGRIFFSKONTROLLE 61

4.1 Methoden 61
4.1.1 Verhinderung eines unberechtigten Datenzugriffs 61
4.1.2 Einmal-Passwort 62
4.1.3 Das Netzwerk-Konto 62
4.1.4 Zugang zum Netzwerk-Konto 63
4.1.5 Biometrische Verfahren 63

4.2 Passwort-Verwaltung 64
4.2.1 Richtlinien für Ihr Passwort 64
4.2.2 Funktion und Grenzen einer Passwort-Verwaltung 66

5 SICHERE WEB-NUTZUNG 67

5.1 Browser-Einstellungen 67
5.1.1 Automatische Vervollständigung bei Dateneingabe 68
5.1.2 Persönliche Daten löschen 69

5.2 Sicheres Surfen 69
5.2.1 Online-Aktivitäten nur auf sicheren Webseiten 70
5.2.2 Vertrauenswürdigkeit einer Website 70
5.2.3 Pharming 72
5.2.4 Software zur Inhaltskontrolle 72

Wissens-Check 77

6 KOMMUNIKATION 79

6.1 E-Mail 79
6.1.1 Warum bei E-Mail eine Verschlüsselung sinnvoll ist 79
6.1.2 Digitale Signatur 81
6.1.3 Gefährliche und unerwünschte E-Mails 82
6.1.4 Merkmale von Phishing 83
6.1.5 Phishing-Attacken melden 86
6.1.6 Gefahr durch Malware 86

6.2 Soziale Netzwerke 88
6.2.1 Vertrauliche oder personenbezogene Informationen 88
6.2.2 Konto-Einstellungen einrichten und regelmäßig überprüfen 88
6.2.3 Konto-Einstellungen in sozialen Netzwerken 89
6.2.4 Gefahren bei der Nutzung von sozialen Netzwerken 90
6.2.5 Missbräuchliche Verwendung oder Fehlverhalten melden 91

6.3 VoIP und Instant Messaging 92
6.3.1 Schwachstellen von Instant Messaging (IM) und Voice over Internet Protocol (VoIP) 92
6.3.2 Methoden beim Gebrauch von IM und VoIP 93

6.4 Mobile Geräte 94
6.4.1 Folgen bei Verwendung von Anwendungen aus inoffiziellen App-Stores 94
6.4.2 App-Berechtigungen.....95
6.4.3 Auslesen privater Informationen aus mobilen Geräten.....96

Wissens-Check..... 98

7 SICHERE DATEN-VERWALTUNG 99

7.1 Daten sichern und Backups erstellen 99
7.1.1 Physischen Sicherung von Computern und mobilen Geräten.....99
7.1.2 Sicherungskopie nützen bei Datenverlust.....100
7.1.3 Konzept zur Datensicherung 100
7.1.4 Dateiversionsverlauf in Windows 10 und Windows 11 101
7.1.5 Backup erstellen.....103
7.1.6 Daten von einem Backup wiederherstellen (Restore) 104

7.2 Abhanden gekommene Geräte 105
7.2.1 Ortung und Sperre über das Internet. 105

7.3 Daten sicher löschen und vernichten..... 107
7.3.1 Unterschied zwischen Löschung von Daten und Vernichtung von Daten 107
7.3.2 Endgültige Löschung / Vernichtung von Daten 108
7.3.3 Löschen von Inhalten muss nicht endgültig sein.....108
7.3.4 Methoden zur endgültigen Datenvernichtung 109

7.4 Datenschutz-Grundverordnung (DSGVO) 110
7.4.1 Zielsetzung 111

7.5 Sicherheit im Homeoffice 111
7.5.1 Tipps zur Absicherung im Homeoffice 112
7.5.2 Sicherer Kommunikationskanal.....113

Wissens-Check..... 114

GLOSSAR 115

Finden Sie die Lösung 126

ANHANG 127

INDEX 129

Einleitung

Um die Sicherheit im Umgang mit EDV zu gewährleisten, ist von allen Anwendenden grundlegendes Wissen über eine sichere Nutzung der Informations- und Kommunikationstechnik (IKT) im Alltag gefordert. Das beinhaltet Kenntnisse über geeignete Maßnahmen für eine sichere Verbindung zu einem Netzwerk, über Sicherheit im Internet und über die richtige Handhabung von Daten und Informationen – mit dem Ziel, die IKT sicher anwenden zu können und sicherheitsspezifischen Herausforderungen der IKT gewachsen zu sein.

So gesehen sollten alle Anwenderinnen und Anwender

- verstehen, wie wichtig die Sicherheit von Daten und Informationen ist und die Grundsätze zum Datenschutz, zur Datenspeicherung, zur Datenkontrolle und zum Schutz der Privatsphäre kennen,
- Bedrohungen für die persönliche Sicherheit durch Identitätsdiebstahl sowie die mögliche Gefährdung von Daten durch Cloud-Computing kennen,
- Passwörter und Verschlüsselung zur Sicherung von Dateien und Daten einsetzen können,
- die Bedrohung durch Malware verstehen und Computer, mobile Geräte und Netzwerke vor Malware schützen sowie auf Malware-Attacken richtig reagieren können,
- übliche Sicherheitsmerkmale von Netzwerken und Drahtlosverbindungen kennen und Personal Firewalls und Persönliche Hotspots verwenden können,
- Computer und mobile Geräte vor unberechtigtem Zugriff schützen und Passwörter sicher handhaben und ändern können,
- geeignete Webbrowser-Einstellungen verwenden können und wissen, wie man die Vertrauenswürdigkeit einer Website feststellt und sicher im Internet surft,
- verstehen, dass Sicherheitsprobleme bei der Kommunikation per E-Mail, VoIP, Instant Messaging und in sozialen Netzwerken sowie durch die Nutzung mobiler Geräte auftreten können,
- Daten auf lokalen Speicherorten und in der Cloud sichern und wiederherstellen können sowie Daten sicher löschen und Geräte entsorgen können.