BHE-zertifizierte Cyber-Security	5
Allgemeines.....	5
Vorteile für Fachfirmen.....	5
BHE-Cyber-Security-Beauftragter (2-tätiger Zertifizierungslehrgang).....	5
1. Normen und Richtlinien in Verbindung mit Netzwerktechnik	7
1.1 Dienstleistungen/Sonstige.....	7
1.2 Netzwerktechnik.....	7
1.3 Einbruchmeldeanlagen.....	7
1.4 Übertragungstechnik.....	7
1.5 Blitz- und Überspannungsschutz.....	8
2. Netzformen Grundstruktur und Bauteile	9
2.1 Grundstrukturen Übersicht.....	9
2.2 LAN (Local Area Network).....	12
2.3 Netzwerkprotokolle.....	23
2.4 Einführung in NAC – PKI – EAP - ACME.....	24
2.5 Wireless Local Area Network bzw. WLAN.....	26
2.6 Mobilfunk.....	32
3. Kabelanlagen	34
3.1 Allgemeines.....	34
3.2 Frühere Kabelsysteme.....	35
3.3 Heutige Kabelsysteme.....	35
3.4 Strukturaufbau heutiger Kabelanlagen.....	38
3.5 Kabeltypen (Kupfer / Licht).....	40
3.6 Verlegungsarten.....	48
3.7 Anschlüsse Kupfer.....	49
3.8 Anschlüsse Licht.....	52
3.9 Testmöglichkeiten und Fehlersuche (Messgerät Empfehlung BHE).....	54
4. Hardware	64
4.1 „Rechnerarchitektur“ allgemein.....	64
4.2 Server.....	64
4.3 Massenspeicher und deren Schnittstellen.....	70
4.4 Clients / Thin-Clients.....	76
4.5 Mobile Geräte.....	77
4.6 Ein-/Ausgabegeräte – Überblick.....	79
4.7 USV – unterbrechungsfreie Stromversorgung.....	84
4.8 Power over Ethernet (PoE).....	87
4.9 Router / WLAN-Router / Mesh WLAN.....	89
5. Software	92
5.1 Betriebssysteme.....	92
5.2 Empfehlungen zur Verwendung von Updates in Sicherheitssystemen.....	95
5.3 Installation von Programmen/Datenbanken.....	95
5.4 Zugriff von „außen“ auf ein IT-System.....	97
5.5 Kommandozeileninterpreter.....	101
5.6 Dateisysteme, Partitionierung, Imaging.....	104
5.7 Verschlüsselung von Daten/Kryptografie.....	108
5.8 Künstliche Intelligenz (KI).....	118

6. IT-Abteilung, Administration	122
6.1 Allgemeines.....	122
6.2 Dokumentation.....	123
6.3 Datenintegrität.....	126
6.4 Datenhaltung.....	126
7. Passwörter	128
7.1 Passwortrichtlinie.....	128
7.2 Sicherer Passwortaufbau.....	129
8. Schutz vor Schadsoftware (Viren, Trojaner und Co.)	133
8.1 Firewall.....	133
8.2 Virens Scanner und Virenschutz.....	135
8.3 Cyber Security bei Videoanlagen.....	137
8.4 Neue Herausforderungen.....	144
8.5 Was versteht man unter dem Begriff „Cyber-Security“?.....	145
8.6 Künstliche Intelligenz (KI) in der Cyber-Security.....	149
9. Verfügbarkeit und Redundanz	150
9.1 Hochverfügbarkeit.....	150
9.2 Redundanzen über Mobilfunk.....	164
10. Datenschutz (EU-Datenschutz-Grundverordnung)	166
10.1 Allgemeines.....	166
10.2 Datenschutzkonforme Datenverarbeitung.....	166
10.3 Dokumentationspflichten.....	166
10.4 Informationspflichten.....	167
10.5 Meldepflichten bei Datenpannen.....	167
10.6 Datenschutz-Folgenabschätzung.....	167
10.7 Pflicht zur Bestellung von Datenschutzbeauftragten.....	167
10.8 Beschäftigtendatenschutz.....	168
10.9 Maßnahmen der Aufsichtsbehörden.....	168
10.10 Bußgelder.....	168
10.11 Schadensersatzansprüche der Betroffenen.....	168
10.12 BHE-Datenschutz-Management-Software.....	169
11. Rechtsgrundlagen	170
11.1 Rechtliche Aspekte allgemein.....	170
11.2 Zugriff auf fremde Netze.....	170
11.3 Rechtliche Aspekte Video.....	171
12. Wichtige Hinweise zur IT-Organisation im Errichter-Betrieb	179
12.1 Allgemeines.....	179
12.2 Die 10 wichtigsten Schritte.....	179
12.3 IT-Notfallmanagement (Muster).....	181
13. Begriffe	184
14. Quellen und weiterführende Informationen	197