

KRITIS

Anforderungen, Pflichten, Nachweisprüfung

DAS INHALTS- VERZEICHNIS

» Hier geht's
direkt
zum Buch

Inhalt

Materialien zum Buch	13
Einleitung	15
Wie Ihnen dieses Buch helfen kann – und was es nicht ist	17
Der Weg durch das Buch	19
Danksagung	23

TEIL I Gesetzliche Anforderungen und Begriffe im KRITIS-Umfeld

1 Geschichtliche Hintergründe zur Nachweisprüfung 29

1.1 UP KRITIS	42
1.2 Das IT-Sicherheitsgesetz von 2015	47
1.2.1 Änderungen im BSIG	49
1.2.2 Änderungen im Energiewirtschaftsgesetz (EnWG)	58
1.3 Das Gesetz zur Umsetzung der NIS-Richtlinie	60
1.4 Das IT-Sicherheitsgesetz 2.0	64
1.4.1 Änderungen im BSIG	64
1.4.2 Änderungen im EnWG	70
1.5 Die NIS-2-Richtlinie	72
1.6 Das BSI-Gesetz (BSIG)	75

2 Die Kritisverordnung 81

2.1 Kritische Infrastrukturen	81
2.2 Die Erarbeitung der Kritisverordnung	82
2.3 Begriffe und Definitionen	84
2.4 Sektoren nach dem BSIG	87
2.4.1 Der Sektor Energie	88
2.4.2 Der Sektor Wasser	90

2.4.3	Der Sektor Ernährung	93
2.4.4	Sektor Informationstechnik und Telekommunikation	94
2.4.5	Sektor Gesundheit	94
2.4.6	Sektor Finanz- und Versicherungswesen	96
2.4.7	Sektor Transport und Verkehr	98
2.4.8	Sektor Siedlungsabfallentsorgung	99
2.5	Anlagenkategorien für kritische Dienstleistungen	101
2.6	Anhänge zu den Sektoren	102
2.6.1	Teil 1 – Grundsätze und Fristen (Kritische Anlagen)	103
2.6.2	Teil 2 – Berechnungsformeln für die kritische Dienstleistung	104
2.6.3	Teil 3 – Anlagenkategorien und Schwellenwerte	108
2.7	Welche Betreiber fallen unter das BSIG?	112
2.8	Unternehmen im besonderen öffentlichen Interesse (UBIs)	114

3 Die IT-Sicherheitskataloge (IT-SiKat) für den Sektor Energie 117

3.1	Die Bundesnetzagentur (BNetzA)	119
3.2	Das Energiewirtschaftsgesetz (EnWG)	120
3.3	Die IT-Sicherheitskataloge	122
3.3.1	Der IT-Sicherheitskatalog für Strom- und Gasnetze (2015)	123
3.3.2	Der IT-Sicherheitskatalog für Energieanlagen (2018)	126
3.4	Die ISO/IEC 27019 – Steuerungssysteme der Energieversorgung	130
3.4.1	Fazit zu Teil 1 des Buches	133

TEIL II Bedeutung und Verantwortung des BSI für Kritische Infrastrukturen

4 Die Unterstützung durch das BSI 137

4.1	Die Gewährleistungsverantwortung gegenüber der Bevölkerung	143
4.2	Die Meldestelle für Informationssicherheitsvorfälle	144

4.3	Erstellung von Lagebildern und Weiterleitung von Information an die KRITIS-Betreiber	145
4.3.1	Die E-Mail-Verkehrsstatistik	147
4.3.2	Die Malware-Statistik	149
4.4	Informations- und Meldeflüsse nach dem BSIG	152
4.4.1	Cyber-Sicherheitswarnungen	153
4.4.2	CERT-Bund Meldungen	154
4.4.3	Die Allianz für Cyber-Sicherheit (ACS)	155
4.4.4	Konferenzen mit BSI-Beteiligung	156

5 Die Orientierungshilfen (OH) des BSI 159

5.1	OH zum Aufbau eines branchenspezifischen Sicherheitsstandards (B3S)	159
5.2	OH zu Systemen zur Angriffserkennung (Sza)	161
5.3	OH zu Nachweisen (für Prüfer)	163

6 Vorgaben an die Art und Weise von Nachweisprüfungen 169

6.1	Registrierung als KRITIS-Betreiber	171
6.2	Das Melde- und Informationsportal (MIP)	171
6.2.1	Schritt 1: Die Institutions-ID	172
6.2.2	Schritt 2: Die Institutionsverwalter-ID	172
6.2.3	Schritt 3: Für die Meldestelle KRITIS registrieren	173
6.2.4	Schritt 4: Sektor und Anlagenkategorie eintragen	173
6.2.5	Schritt 5: Meldeberechtigte ergänzen	173
6.2.6	Token	174
6.2.7	Sanitarisierung	174
6.2.8	Die Aufgaben der Meldeberechtigten	174
6.3	Der Nachweisprozess	176
6.4	Die Vorgabedokumente im Nachweisprozess	177
6.4.1	Grundsätzliche Anforderungen im Nachweisprozess (GAiN)	177
6.4.2	Das Nachweisdokument KI für KRITIS-Betreiber	181
6.4.3	Der Prüfplan als Excel-Vorlage für Auditoren	182
6.4.4	Das Nachweisdokument P für Prüfer	184

6.4.5	Die Nachweisdokumente KI* / P* für Prüfungen im Sektor Energie	187
6.4.6	Selbsterklärung der prüfenden Stelle	189
6.4.7	Selbsterklärung zur zusätzlichen Prüfverfahrenskompetenz	190
6.4.8	Erklärung zur Unabhängigkeit	191
6.4.9	Selbsterklärung für AWW-UBI (UBI 1)	192
6.4.10	Die Mängelliste als Excel-Vorlage für Auditoren	194

TEIL III Pflichten und Möglichkeiten des KRITIS-Betreibers

7 Ihre Pflichten als KRITIS-Betreiber 199

7.1	Der Geltungsbereich für die kritische Dienstleistung	200
7.1.1	Den KRITIS-Geltungsbereich eingrenzen	201
7.1.2	Den Netzstrukturplan erstellen	203
7.1.3	Ein zu kleiner Geltungsbereich	205
7.1.4	Ein zu großer Geltungsbereich	206
7.1.5	Der Geltungsbereich umfasst die kritische Dienstleistung	208
7.1.6	Gruppierung von Objekten im Netzstrukturplan	210
7.2	Organisatorische und technische Vorkehrungen zur Vermeidung von Störungen	210
7.2.1	Berücksichtigung des All-Gefahrenansatzes	211
7.2.2	Eingeschränkte Risikoakzeptanz	212
7.2.3	Maßnahmen nach dem Stand der Technik	213
7.2.4	Umsetzung aller risikomindernden Maßnahmen	214
7.3	Systeme zur Angriffserkennung (SzA)	215
7.3.1	Die Umsetzungsempfehlungen des BSI zu SzA	216
7.3.2	Praktisches Umsetzungsbeispiel IRMA®	219
7.3.3	Besonderheiten des Energie-Sektors	221
7.4	Interne Audits	222
7.5	Melden von Informationssicherheitsvorfällen, Störungen und Ausfällen	223
7.6	Gemeinsame übergeordnete Ansprechstelle (GÜAS)	224

8 Einen branchenspezifischen Sicherheitsstandard (B3S) veröffentlichen 227

8.1	Aufbau eines B3S mithilfe der OH B3S	227
8.2	Einen B3S beim BSI einreichen	232
8.3	Eignungsfeststellung des BSI	235
8.4	Aktuell veröffentlichte B3S	236
8.5	Vorteile und Nachteile vorhandener B3S	238

TEIL IV Die Nachweisprüfung gemäß § 8a Abs. 3 BSIG

9 Planung der Nachweisprüfung durch den Betreiber 241

9.1	Auswahl einer Prüfstelle	241
9.2	Anforderungen an eine prüfende Stelle	242
9.3	Eignung als prüfende Stelle	243

10 Vorarbeiten für die Nachweisprüfung durch Prüfer 247

10.1	Welche Prüfgrundlagen können wir einsetzen?	248
10.1.1	Ein passender B3S als Prüfgrundlage	250
10.1.2	Klassische Standards als Prüfgrundlage	251
10.1.3	Cloud Computing Compliance Criteria Catalogue – C5:2020	252
10.1.4	Die »Konkretisierten Anforderungen« als Prüfgrundlage	253
10.1.5	Die Orientierungshilfe B3S als Prüfgrundlage	254
10.1.6	Der IT-Sicherheitskatalog als Prüfgrundlage	256
10.2	Kompetenzbereiche und Aufteilung im Prüftteam	257
10.3	Fachexperten auswählen und einsetzen	258
10.4	Die Prüfungsplanung durch die Prüfstelle	260
10.4.1	Abstimmung im Vorfeld	260
10.4.2	Einen Prüfplan entwerfen	260
10.4.3	Die Excel-Vorlage des BSI zum Prüfplan	261

10.5 Auswahl von Stichproben	264
10.6 Berücksichtigung externer Dienstleister	266
10.7 Die Mängelkategorien des BSI	267

11 Die Nachweisprüfung durchführen 271

11.1 Audit von Managementsystemen nach der ISO 19011	272
11.1.1 Das Eröffnungsgespräch	273
11.2 Arbeitsschutz für Auditoren	275
11.3 Remote-Audits	277
11.3.1 Welche Risiken können sich bei einem Remote-Audit ergeben?	277
11.3.2 Themen für Remote-Audits	278
11.4 Mögliche Prüfmethode	282
11.5 Verwendung bestehender Zertifikate	283
11.6 Prüfung der branchenspezifischen Maßnahmen	287
11.7 Prüfung des BCMS	291
11.7.1 Organisation zum BCMS	293
11.7.2 Vorbereitung und Durchführung von Notfallübungen	294
11.7.3 Wartungen, Inspektionen und Wiederherstellung	296
11.8 Aktualität der BSI-Formulare und OHs beim Prüfteam	297

12 Nacharbeiten nach der Nachweisprüfung 301

12.1 Aufgaben des Prüfers	302
12.1.1 Bewertung des ISMS-Reifegrades	302
12.1.2 Bewertung des BCMS-Reifegrades	303
12.1.3 Bewertung des SzA-Umsetzungsgrades	304
12.1.4 Die Mängelliste dokumentieren	310
12.1.5 Übermittlung der Auditdokumentation an den Betreiber	315
12.2 Aufgaben des Betreibers	316
12.2.1 Nachverfolgung und Überwachung der geplanten Maßnahmen	317
12.2.2 Selbsterklärung der AWW-UBI (UBI 1)	317
12.2.3 Fristen für Betreiber	319
12.2.4 Übergabe der Nachweise an das BSI	324
12.2.5 Übergabe der Nachweise im Energie-Sektor	325

13 Prüfung der eingereichten Nachweise durch das BSI 329

13.1	Nachforderung von Dokumenten	329
13.2	Eskalation bei Unvollständigkeit	331
13.3	Sonderprüfungen nach dem BSIG	332
13.4	Nachprüfung wegen zu kleinem Geltungsbereich	333
13.5	Bußgelder	334

TEIL V Aus der Praxis – in die Praxis

14 Untersuchung zu Umfang und Komplexität der Nachweisprüfung 341

14.1	Die BSI-Studie zur Umsetzung der IT-Sicherheitsgesetze	342
14.2	Studie zu Nachweisprüfungen nach BSIG	344
14.2.1	Durchführung der Umfrage	345
14.2.2	Ziele der Umfrage	345
14.2.3	Statistische Auswertung und Ergebnisse	347
14.2.4	Fazit der Ergebnisse	372

15 Zusätzliche Prüfverfahrenskompetenz nach dem BSIG 377

15.1	Weiterbildung und schriftliche Prüfung	377
15.2	Überprüfung Ihrer Antworten	378

16 Fazit und Ausblick 385

Literaturverzeichnis	389
Index	395