Krisen, KRITIS & Datenschutz

CAMPUS TAGE

www.campustage.org

dsn Aka demie

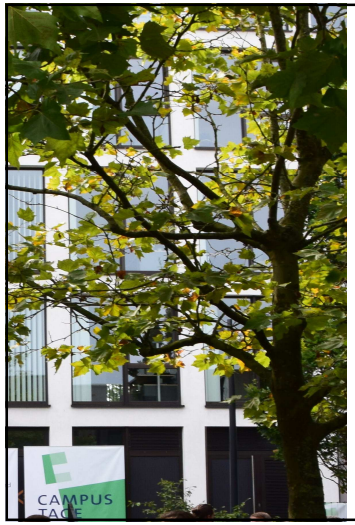
---

dsn Aka demie

Von divergierenden und konvergierenden Anforderungen

CAMPUSTAGE 2023

www.datenschutz-cert.de



dsn Aka demie

Dr. Sönke Maseberg
Geschäftsführer datenschutz cert GmbH

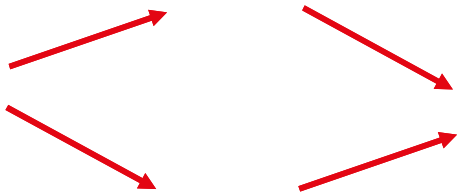
datenschutz cert GmbH
T +49(0)421 69 66 32 552
E-Mail smaseberg@datenschutz-cert.de

www.datenschutz-cert.de

Von divergierenden und konvergierenden Anforderungen

dsn Aka demie

Divergenz *Konvergenz*



Aktivitäten

IT-Sicherheits-katalog

BNetzA

§ 11 Abs. 1a EnWG: Strom- und Gas-netzbetreiber

§ 11 Abs. 1b EnWG: Energieanlagen-betreiber

Bundesamt für Sicherheit in der Informationstechnik

KRITIS-VO

§ 8a BSIG

Informationssicherheit – Stand der Technik

Nachweise ggü. BSI

alle 2 Jahre

Prüfer

Prüfende Stellen

SzA

ISO/IEC 27001

ISO/IEC 27019

ISO 27001 auf der Basis von IT-Grundschutz

Divergenz

Agenda

- § 8a BSIG / KRITIS-VO
- ISO/IEC 27001
- IT-Grundschutz
- IT-Sicherheitskataloge
- Systeme zur Angriffserkennung
- Konvergenz
- Fazit

§ 8a BSIG

§ 8a Sicherheit in der Informationstechnik Kritischer Infrastrukturen

(1) Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens bis zum ersten Werktag, der darauf folgt, dass diese erstmalig oder erneut als Betreiber einer Kritischen Infrastruktur nach der Rechtsverordnung nach § 10 Absatz 1 gelten, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei soll der Stand der Technik eingehalten werden. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.

KRITIS-VO

KRITIS-Schwellenwerte

1.1.1	Erzeugungsanlage	Installierte	104
1.2	Stromübertragung		
1.2.1	Übertragungsnetz	Durch Letztverbraucher und Weiterverteiler entnommene Jahresarbeit in GWh/Jahr	3 700
3.3.2	Tankstellennetz	Verteilter Kraftstoff in Tonnen/Jahr oder	420 000
2.1	Housing		
2.1.1	Rechenzentrum (Housing)	Vertraglich vereinbarte Leistung in MW	3,5
		vom 20. Mai 2020,	
3.3.1	Apotheke	Abgegebene Packungen/ Jahr	4 650 000

§ 8a-Nachweise: Alle zwei Jahre

(3) Betreiber Kritischer Infrastrukturen haben die Erfüllung der Anforderungen nach den Absätzen 1 und 1a spätestens zwei Jahre nach dem in Absatz 1 genannten Zeitpunkt und anschließend alle zwei Jahre dem Bundesamt nachzuweisen. Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen. Die Betreiber übermitteln dem Bundesamt die Ergebnisse der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel. Das Bundesamt kann die Vorlage der

§ 8a-Nachweise: Prüfer

PS.6 Angaben zum Prüfteam – Zusammensetzung und Abdeckung aller Kompetenzbereiche

Prüfer				Kompetenzbereiche			Zusätzliche Prüfverfahrens-kompetenz	
Nr.	Name, Vorname	Organisation	Prüf-anteil in %	Audit	IT-Sicher heit	Bran-che	Zusatz-qualifi-kation	Gleich-wertige Komp.
1								
2								

§ 8a-Nachweise: Prüfende Stelle

PS.3 Angaben zur Eignung der prüfenden Stelle

- ☒ DAkkS-Akkreditierung[10]
- ☒ Zertifizierung als IT-Sicherheitsdienstleister beim BSI
- ☒ Anerkennung als Prüfstelle beim BSI
- ☒ Interne Revision mit Quality Assessment nach IDW PS 983 oder DIIR Revisions-standard Nr. 3[1]
- ☒ Wirtschaftsprüfer/Wirtschaftsprüfungsgesellschaft[10]
- ☒ Selbsterklärung gegenüber dem BSI

§ 8a-Nachweis: Standard

PD.2 Angaben zur Art der durchgeführten Prüfung

Die Überprüfung der Umsetzung von § 8a Absatz 1 BSIG wurde

- ☒ als eigenständige Prüfung durchgeführt.
- ☒ als Zusatz zu einer anderen Prüfung durchgeführt. *(Zutreffendes bitte ankreuzen)*
  - ☒ ISO 27001-Zertifizierung auf Basis von IT-Grundschutz [4,5]
  - ☒ ISO 27001-Zertifizierungsverfahren (nativ)[5]
  - ☒ unternehmensinternes Sicherheitsaudit
  - ☒ Wirtschaftsprüfung
- ☒ als sonstige Prüfung durchgeführt. *(bitte erläutern)*

B3S

Dauer der Gesamtprüfung in Personen-Prüftagen
(falls als Zusatz- oder sonstige Prüfung durchgeführt)

Branchen-spezifische Sicherheits-standards (B3S)

B3S im Sektor Energie
- Branchenspezifischer Sicherheitsstandard für Anlagen oder Systeme zur Steuerung/Bündelung elektrischer Leistung (B3S Aggregatoren)
- Branchenspezifischer Sicherheitsstandard (B3S) für die Verteilung von Fernwärme (Fernwärmenetze)

B3S im Sektor Wasser
- Branchenspezifischer Sicherheitsstandard Wasser/Abwasser

B3S im Sektor Ernährung
- Sicherheitsstandard für die Ernährungsindustrie
- B3S für den Lebensmittelhandel

B3S im Sektor IT und Telekommunikation
- Branchenspezifischer Sicherheitsstandard (B3S) für Housing, Hosting und CDN

B3S im Sektor Gesundheit
- Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus

B3S im Sektor Finanz- und Versicherungswesen
- Branchenspezifischer Sicherheitsstandard für gesetzliche Kranken- und Pflegeversicherer
- Branchenspezifischer Sicherheitsstandard des Bundesverbandes der electronic cash-Netzbetreiber
- B3S Allianz Deutschland AG

B3S im Sektor Transport und Verkehr
- Branchenspezifischer Sicherheitsstandard für die Verkehrssteuerungs- und Leitsysteme im kommunalen Straßenverkehr
- Branchenspezifischer Sicherheitsstandard für die Verkehrssteuerungs- und Leitsysteme der Bundesautobahn

ISO/IEC 27001

weltweiter Standard zur Informationssicherheit

internationale Community (International Accreditation Forum IAF)

Akkreditierungsstellen (in Deutschland: DAkkS)

Zertifizierungsstellen

Auditoren

Zertifikatslaufzeit: 3 Jahre

NEIN! ISO/IEC 27001 nicht ausreichend als § 8a-Nachweis

Authentizität als Sicherheitsziel

Risikobehandlung: keine Versicherung, keine Übernahme, kein Ausschluss von KRITIS-Bereichen

Formulare

ISO 27001 auf der Basis von IT-Grundschutz

Standard zur Informationssicherheit

Zertifizierungsstelle: BSI

Auditoren

Zertifikatslaufzeit: 3 Jahre

IT-Grundschutz auch nicht ausreichend als § 8a-Nachweis

Authentizität als Sicherheitsziel

Risikobehandlung: keine Versicherung, keine Übernahme, kein Ausschluss von KRITIS-Bereichen

Formulare

IT-Sicherheitskatalog gem. § 11 Abs. 1a EnWG
(Strom- und Gasnetzbetreiber)

gilt für alle – unabhängig von Schwellenwerten

Akkreditiı
akkreditie
Standard:
Besonder
Auditorer
Zertifikat

1.2	Stromübertragung		
1.2.1	Übertragungsnetz	Durch Letztverbraucher und Weiterverteiler entnommene Jahresarbeit in GWh/Jahr	3 700
1.3	Stromverteilung		
1.3.1	Stromverteilernetz	Durch Letztverbraucher und Weiterverteiler entnommene Jahresarbeit in GWh/Jahr	3 700

statt § 8a BSIG-Nachweis

IT-Sicherheitskatalog gem. § 11 Abs. 1b EnWG
(Energieanlagenbetreiber)

abhängig von Schwellenwerten

Akkreditierun
akkreditierte
Standard: ISO
Besonderheit
Auditoren
Zertifikatsgül
statt § 8a BSIC

1.1.1	Erzeugungsanlage	Installierte Nettonennleistung (elektrisch oder direkt mit Wärmeauskopplung verbundene elektrische Wirkleistung bei Wärmenennleistung ohne Kondensationsanteil) in MW oder	104
		installierte Nettonennleistung in MW, wenn die Anlage als Schwarzstartanlage nach § 3 Absatz 2 des Beschlusses der Bundesnetzagentur vom 20. Mai 2020, Aktenzeichen BK6-18-249 kontrahiert ist, oder	0

Systeme zur Angriffserkennung
(SzA)

(1a) Die Verpflichtung nach Absatz 1 Satz 1, angemessene organisatorische und technische Vorkehrungen zu treffen, umfasst ab dem 1. Mai 2023 auch den Einsatz von Systemen zur Angriffserkennung. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen. Absatz 1 Satz 2 und 3 gilt entsprechend.

Einführung SzA bis: 01.05.2023

Nachweis ggü. BSI

- Netzbetreiber erstmals zum 01.05.2023, dann alle 2 J.
- Kraftwerksbetreiber, die unter KRITIS fallen: dito

KRITIS-Betreiber: reguläre § 8a-Nachweispflichten

Konvergenz

Ziel: Informationssicherheit nach Stand der Technik
=Informationssicherheits-Managementsystem (ISMS)

anerkannte Stellen
unabhängige Prüfungen
anerkannte Prüfer
anerkannte Standards
harmonisierte Laufzeiten
fokussierte Inhalte

Konvergenz

KRITIS-Dachgesetz
(DachG)

GESETZ · 28.07.2023

Entwurf eines Gesetzes zur Umsetzung der CER-Richtlinie und zur Stärkung der Resilienz kritischer Anlagen

"Erstmalige bundeseinheitliche Regelungen für den physischen Schutz kritischer Infrastrukturen sollen die Resilienz der Wirtschaft und dadurch auch die Versorgungssicherheit der Bevölkerung stärken."

Bundesministerium
des Innern
und für Heimat

Fazit

- Gefährdungslage für Kritische Infrastrukturen ist hoch
- Harmonisierung der staatlichen Vorgaben
- unabhängige Prüfungen
- einheitliche Standards
- Abbau Bürokratie

Aufsatz: DuD 2023, 541

Seminare
Webinare
eLearning

Datenschutz und
Informationssicherheit

Vielen Dank für Ihre Aufmerksamkeit!

Konsul-Smidt-Straße 88 • 28217 Bremen
T +49 (0) 421 69 66 32-298
Mail: akademie@dsn-group.de

www.dsn-group.de