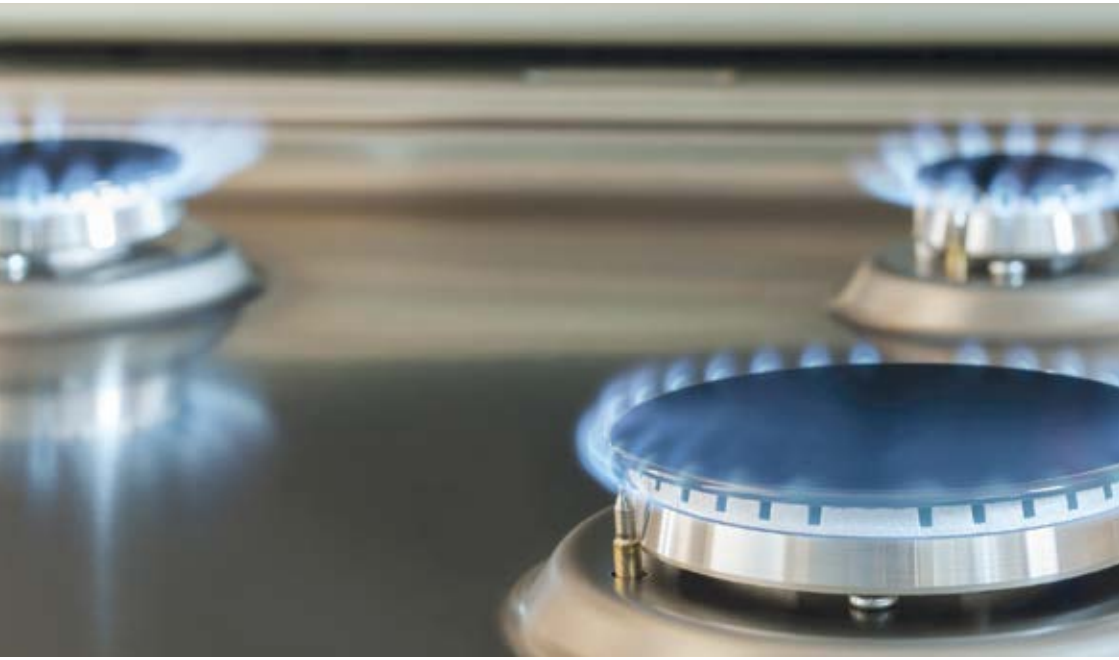

Zertifizierung von Netzbetreibern nach

IT-Sicherheitskatalog gemäß § 11 Abs. 1a EnWG

datenschutz cert

ISO/IEC 27001

ISO/IEC 27001 ist der **internationale Standard für Informationssicherheit.** Er behandelt Anforderungen an ein sogenanntes **Informationssicherheits-Managementsystem (ISMS),** also an die Prozesse in einer Organisation, um Informationssicherheit dauerhaft zu etablieren und aufrechtzuerhalten.

Ob das so ist, kann von unabhängigen Auditoren überprüft und durch ein Zertifikat nach außen dokumentiert werden – etwa um **gesetzlichen Anforderungen** nachzukommen: Mit dem „IT-Sicherheitskatalog gem. § 11 Abs. 1 a Energiewirtschaftsgesetz“ der Bundesnetzagentur (BNetzA) hat der Gesetzgeber beispielsweise Vorgaben **für Netzbetreiber** erlassen. Hintergrund ist die zunehmende Durchdringung vormals getrennter Versorgungsnetze mit IT-Infrastrukturen. Denn im Hinblick auf die für die Gesellschaft wichtige Versorgung bekommt Informationssicherheit einen neuen Stellenwert. Und besonders nachprüfbare Sicherheit.

Der IT-Sicherheitskatalog fordert: „Netzbetreiber [haben] ein ISMS zu implementieren, das den Anforderungen der DIN ISO/IEC 27001 [...] genügt und mindestens die unter Abschnitt D beschriebenen Systeme, d.h. Telekommunikations- und EDV-Systeme, die für einen sicheren Netzbetrieb notwendig sind, umfasst.“

Und an dieser Stelle können wir Sie unterstützen: Die datenschutz cert GmbH ist bei der Deutschen Akkreditierungsstelle (DAkkS) akkreditiert.

Sprechen Sie uns an. Wir freuen uns auf Sie!

Für wen gilt der IT-Sicherheitskatalog?

Der IT-Sicherheitskatalog gilt für alle **Betreiber eines Energieversorgungsnetzes in den Bereichen Strom und Gas;** ausgenommen sind nur kleine Betreiber.

Im Fokus stehen die **TK- und IT-Systeme,** die für den **sicheren Netzbetrieb notwendig** sind. Der **Netzbetreiber bleibt verantwortlich,** auch wenn er Teilaspekte als Outsourcing in Anspruch nimmt.

Welche Anforderungen sind zu beachten?

Geltungsbereich:

Der Scope muss alle Anwendungen, Systeme und Komponenten enthalten, die für einen sicheren Netzbetrieb notwendig sind. Damit sind insbesondere alle Systeme des Netzbetreibers vom Scope erfasst, welche direkt Teil der Netzsteuerung sind, d. h. unmittelbar Einfluss auf die Netzfahrweise nehmen.

ISMS:

Ein Informationssicherheits-Managementsystems (ISMS) ist einzuführen. Zu berücksichtigen ist neben der ISO/IEC 27001 die branchenspezifische Norm ISO/IEC 27019.

Risikoanalyse:

- Schutzziele: Verfügbarkeit, Integrität und Vertraulichkeit
- Schadenskategorien: „kritisch“, „hoch“, „mäßig“
- Einstufung: Komponenten, Systeme und Anwendungen, die für einen sicheren Netzbetrieb notwendig sind, als mindestens „hoch“
- Beachtung besonderer Schadensszenarien

Netzstrukturplan:

- alle Anwendungen, Systeme und Komponenten des Geltungsbereiches samt Verbindungen
- insbesondere „Leitsystem/Systembetrieb“, „Übertragungstechnik/Kommunikation“ und „Sekundär-, Automatisierungs- und Fernwirktechnik“

Ansprechpartner IT-Sicherheit:

Der BNetzA muss ein Ansprechpartner gemeldet werden.

Auditierung und Zertifizierung:

Das ISMS muss auditiert und zertifiziert werden. Das Zertifikat muss bis zum 31.01.2018 der BNetzA übermittelt werden.

ISMS – Ganzheitliche Informationssicherheit

Informationssicherheit und Datenschutz sind zwei zentrale Anforderungen der Informationsgesellschaft. Es hat sich gezeigt, dass für eine ganzheitliche Informationssicherheit eine strukturierte Herangehensweise erforderlich ist – durch ein **Informationssicherheits-Managementsystem (ISMS).**

Ein ISMS ist ein Top-Down-Ansatz, um Informationssicherheit in einer Organisation zu etablieren und effizient und wirkungsvoll umzusetzen. Ein ISMS ist ein „lebender" Prozess, in dem das Management regelmäßig über den Zustand des ISMS informiert wird, wodurch das Management seine Verantwortung wahrnehmen und ggf. reagieren kann. Ein ISMS ist skalierbar und auch für größere Organisationen einsetzbar. Der ISMS-Prozess ist auch bekannt als **PDCA-Zyklus: Plan – Do – Check – Act.**

Was tun wir?

Wir **prüfen** und **zertifizieren Informationssicherheit** und **Datenschutz.**

Unsere Kompetenzen

Die Anforderungen an die Energiewirtschaft tangieren viele Standards, Regelwerke und Normen, zu denen wir über umfangreiche Erfahrungen verfügen:

- **IT-Sicherheitskatalog** gemäß § 11 Absatz 1a EnWG
- **ISO/IEC 27001**
- **ISO 27001** auf der Basis von IT-Grundschutz
- **BSI TR-03109-6** für die Smart Meter Gateway Administration
- **Penetrationstests** für Smart Meter Gateway Administratoren als IT-Sicherheitsdienstleister
- **BSI TR-03145 „Secure CA Operation"** für die Smart Meter-PKI

Die datenschutz cert GmbH stellt eines der beiden GS-Zertlabs, die für das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Prüfbegleitung in den IT-Grundschutz-Verfahren durchführt.

Zweistufiges Verfahren

Um Ihnen ein Höchstmaß an Unabhängigkeit zu garantieren, setzen wir auf ein zweistufiges Zertifizierungsverfahren:

1. Der bei der datenschutz cert GmbH lizenzierte Auditor prüft die Konformität des Informationssicherheits-Managementsystems gemäß ISO/IEC 27001 und empfiehlt im Auditreport die Zertifizierung. Es ist möglich, beim Audit nach ISO/IEC 27001 direkt branchenspezifische Anforderungen mit zu begutachten, wie hier zum IT-Sicherheitskatalog.
2. Die Zertifizierungsstelle prüft das Auditverfahren, insbesondere um eine Vergleichbarkeit zwischen den Audits sicher zu stellen. Anschließend kann die Zertifizierung ausgesprochen und das Zertifikat erstellt werden.

Kosten und Aufwand

Kosten und Aufwand für die Auditierung hängen von der Größe und Komplexität des Untersuchungsgegenstands ab. Die für alle akkreditierten Zertifizierungsstellen verbindliche Akkreditierungsnorm gibt dazu folgende Eckdaten bzgl. der Audittage vor, die sich an der Anzahl der Mitarbeiter im Geltungsbereich orientiert:

Anzahl der Mitarbeiter im Geltungsbereich	1–10	11–15	16–25	26–45	46–65	66–85	86–125	...
Anzahl der Tage für die Auditierung vor Ort	5	6	7	8,5	10	11	12	...

Sprechen Sie uns gerne an!
Wir unterbreiten Ihnen ein konkretes Angebot.

Zertifizierungsprozess

Laufzeit des Zertifikats
(i.d.R. 3 Jahre)

ISO

Erst-Zertifizierung

- **Auditierung**
  - Vorbereitung/Sichtung Referenzdokumente
  - Preaudit
  - Audit
  - ausführlicher Report
- **Zertifizierung**
  - Zertifizierungstätigkeit
  - Ausstellung Zertifikat
  - Übergabe des Zertifikats
  - Listung im Internet über gesamte Laufzeit

1. Überwachungsaudit (nach einem Jahr)

2. Überwachungsaudit (nach zwei Jahren)

Re-Zertifizierung

- Auditierung
- Zertifizierung

datenschutz cert GmbH
Ihr Ansprechpartner:
Dr. Sönke Maseberg
+49 (0) 421 69 66 32 50
smaseberg@datenschutz-cert.de

02/dsc

datenschutz cert GmbH

Hauptsitz Bremen
Konsul-Smidt-Straße 88a
28217 Bremen

Niederlassung Berlin-Mitte
Reinhardtstraße 46
10117 Berlin

Tel.: 0421 69 66 32 50
office@datenschutz-cert.de
www.datenschutz-cert.de

Wir sind bei der Deutschen Akkreditierungsstelle (DAkkS) als **Zertifizierungsstelle** akkreditiert.

datenschutz cert

DAkkS
Deutsche
Akkreditierungsstelle
D-ZM-16077-01-00