Unterstützungsleistung durch TELCAT

Durchführung eines Beratungstags / Workshops (als Einstieg in die Thematik). Inhaltliche Aspekte:

- Ziel und Zweck der Regularien
- Konkrete Anforderungen an Betreiber Kritischer Infrastrukturen
- Kurzvorstellung des DIN ISO/IEC 27001 und Erweiterungen
- Bedeutung von ISMS-relevanten Anforderungen (KVP[3], IS[4]-Management, -Organisation, IT-Sicherheitsbeauftragter etc.)
- Wesentliche Bestandteile des Risikomanagements (kritische Geschäftsprozesse, Risikoanalyse/-Behandlung, Notfall-, Krisenmanagement, IT-Sicherheitsrevision etc.)
- Grundlegende organisatorische Maßnahmen (Strukturanalyse, Schutzbedarfsbestimmung, Netzstrukturplan etc.)
- Mögliche Unterstützungsleistungen durch TELCAT
- Notwendige Tätigkeiten, die durch den Betreiber selbst zu bewältigen sind
- Ggf. konkreter Einstieg in die Soll-Ist-Analyse
- Definition der weiteren Vorgehensweise (nächste Schritte, zeitlicher Rahmen)

Weitere Tätigkeiten:

- Unterstützung bei der Umsetzung von organisatorischen und technischen Maßnahmen
- Einführung, Lieferung technischer Produkte (Notfall-, Patch-Management, Firewalls, NAC[5] etc.)
- Übernahme von Tätigkeiten als externer IT-Sicherheitsbeauftragter
- Durchführen von DIN ISO/IEC 27001-Audits

TELCAT MULTICOM GmbH
Sudetenstraße 10
38239 Salzgitter
Germany
Tel.: +49 5341 21-8888
Fax: +49 5341 21-8899

TELCAT
KOMMUNIKATIONSTECHNIK GmbH
Sudetenstraße 10
38239 Salzgitter
Germany
Tel.: +49 5341 21-8877
Fax: +49 5341 21-8440

www.telcat.de
info@telcat.de

IT-Sicherheitsgesetz: Sind Sie vorbereitet?

Wir unterstützen Sie.

TELCAT MULTICOM
Ein Unternehmen der Salzgitter Gruppe

TELCAT MULTICOM
Ein Unternehmen der Salzgitter Gruppe

TMG 06.17

Das IT-Sicherheitsgesetz - Schutz Kritischer Infrastrukturen: Ein Muss für alle Betreiber.

Die Abhängigkeit von digitalen Infrastrukturen und IT-Systemen wächst in nahezu allen Lebensbereichen in unserer Gesellschaft. Damit steigen die Sicherheitsanforderungen an solche Systeme, während gleichzeitig die Bedeutung ihrer Verfügbarkeit zunimmt.

Dem Rechnung tragend hat der Bundestag am 12.06.2015 das neue **IT-Sicherheitsgesetz** zur Erhöhung der Sicherheit informationstechnischer Systeme verabschiedet. Hierin sind verbindliche Anforderungen an die IT-Sicherheit Kritischer Infrastrukturen (Einrichtungen, die für das Gemeinwesen von zentraler Bedeutung sind) konkret formuliert.

Ferner hat die Bundesnetzagentur gemeinsam mit dem BSI[1] einen Katalog mit Sicherheitsanforderungen *Sicherheitskatalog gem. § 11 Abs. 1a EnWG* (Energiewirtschaftsgesetz) zum Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die der Netzsteuerung dienen, erstellt (**IT-Sicherheitskatalog**). Dieser Katalog soll den Betreibern von Energieversorgungsnetzen u. a. als Grundlage für die Implementierung eines ISMS[2] dienen.

Was kommt auf Sie als Betreiber Kritischer Infrastrukturen zu? Worauf müssen Sie sich einstellen?

IT-Sicherheitsgesetz
Mit dem IT-Sicherheitsgesetz werden Mindestanforderungen an die IT-Sicherheit für Kritische Infrastrukturen vorgegeben. Deren Betreiber werden damit verpflichtet,

- angemessene organisatorische und technische Vorkehrungen **spätestens zwei Jahre** nach Inkrafttreten der Rechtsverordnung umzusetzen,
- die Erfüllung dieser Anforderungen **alle zwei Jahre** (z. B. durch Sicherheitsaudits oder Zertifizierungen) mit Übermittlung der Ergebnisse an das BSI nachzuweisen sowie
- erhebliche IT-Sicherheitsvorfälle an das BSI zu melden.

IT-Sicherheitskatalog
Die Anforderungen des Sicherheitskataloges sind künftig von **allen** Netzbetreibern zu erfüllen, soweit sie über Systeme verfügen, die in den Anwendungsbereich des Sicherheitskataloges fallen. Die Umsetzung der Anforderungen hat **spätestens ein Jahr** nach dessen Inkrafttreten zu erfolgen.
Die Netzbetreiber werden damit verpflichtet,

- ein ISMS gemäß DIN ISO/IEC 27001 einzuführen,
- dieses ISMS durch eine unabhängige, hierfür zugelassene Stelle zu zertifizieren und
- einen IT-Sicherheitsbeauftragten als gleichzeitigen Ansprechpartner für die Bundesnetzagentur innerhalb **von zwei Monaten** nach Veröffentlichung des Katalogs zu benennen.

Kritische Infrastrukturen
Gemäß BSI-Gesetz vom 14. August 2009 (BGBl. I, S. 2821) zählen zu Kritischen Infrastrukturen solche Einrichtungen, Anlagen oder Teile davon, die für das Funktionieren des Gemeinwesens von hoher Bedeutung sind. Durch deren Ausfall oder Beeinträchtigung würden nachhaltig wirkende Versorgungsengpässe oder erhebliche Störungen der öffentlichen Sicherheit eintreten. Die folgenden Sektoren sind dabei relevant:

- **Energie** (Elektrizität, Gas, Mineralöl)
  Beispiele: Stadtwerke, Energieversorger
- **Informationstechnik und Telekommunikation** (Telekommunikation, Informationstechnik)
  Beispiele: Mobilfunkanbieter, TK-Service Provider
- **Transport und Verkehr** (Luftfahrt, See-, Binnenschifffahrt, Schienen-, Straßenverkehr, Logistik)
  Beispiele: Verkehrsbetriebe, Kurierdienste, Flughäfen
- **Gesundheit** (Medizinische Versorgung, Arzneimittel und Impfstoffe, Labore)
  Beispiele: Krankenhäuser, Kliniken, Notfalleinrichtungen, medizinische Spezialeinrichtungen
- **Wasser** (Öffentliche Wasser-, Abwasserbeseitigung)
  Beispiele: Stadtwerke, Kraftwerke
- **Ernährung** (Ernährungswirtschaft, Lebensmittelhandel)
  Beispiele: Wirtschaftsbereiche, die sich mit Produktion, Verarbeitung und Handel von Lebensmitteln bzw. Nahrungsmitteln befassen
- **Finanz- und Versicherungswesen** (Banken, Börsen, Versicherungen, Finanzdienstleister)
  Beispiele: Ämter, Sparkassen

1 Bundesamt für Sicherheit in der Informationstechnik
2 Informationssicherheitsmanagementsystem
3 Kontinuierlicher Verbesserungsprozess
4 Informationssicherheit
5 Network Access Control (Netzzugangskontrolle)

Quellen: www.bmi.bund.de und www.bundesnetzagentur.de