Jetzt kaufen auf shop.wvgw.de
Als Print oder PDF-Download

Deutscher Verein des Gas- und Wasserfaches e.V.

DVGW
INFORMATION

www.dvgw-regelwerk.de

DVGW-Information

GAS Nr. 22 März 2017

Informationssicherheit in der Energieversorgung

GAS

in Kooperation mit
FNN FORUM NETZTECHNIK/ NETZBETRIEB IM VDE

Der DVGW mit seinen rund 14.000 Mitgliedern ist der technisch-wissenschaftliche Verein im Gas- und Wasserfach, der seit mehr als 150 Jahren die technischen Standards für eine sichere und zuverlässige Gas- und Wasserversorgung setzt, aktiv den Gedanken- und Informationsaustausch in den Bereichen Gas und Wasser anstößt und durch praxisrelevante Hilfestellungen die Weiterentwicklung im Fach motiviert und fördert.

Der DVGW ist wirtschaftlich unabhängig, politisch neutral und dem Gemeinwohl verpflichtet.

Das DVGW-Regelwerk ist ein zentrales Instrument zur Erfüllung des satzungsgemäßen Zwecks und der Aufgaben des DVGW. Auf Basis der gesetzlichen Bestimmungen werden im DVGW-Regelwerk insbesondere sicherheitstechnische, hygienische, umweltschutzbezogene, gebrauchstauglichkeitsbezogene, verbraucherschutzbezogene und organisatorische Anforderungen an die Versorgung und Verwendung von Gas und Wasser definiert. Mit seinem Regelwerk entspricht der DVGW der Eigenverantwortung, die der Gesetzgeber der Versorgungswirtschaft zugewiesen hat – für technische Sicherheit, Hygiene, Umwelt- und Verbraucherschutz.

Benutzerhinweis

Mit dem DVGW-Regelwerk sind folgende Grundsätze verbunden:

Das DVGW-Regelwerk ist das Ergebnis ehrenamtlicher Tätigkeit, das nach den hierfür geltenden Grundsätzen (DVGW-Satzung, Geschäftsordnung GW 100) erarbeitet worden ist. Für dieses besteht nach der Rechtsprechung eine tatsächliche Vermutung, dass es inhaltlich und fachlich richtig ist.

- Das DVGW-Regelwerk steht jedermann zur Anwendung frei. Eine Pflicht kann sich aus Rechts- oder Verwaltungsvorschriften, einem Vertrag oder sonstigem Rechtsgrund ergeben.
- Durch das Anwenden des DVGW-Regelwerkes entzieht sich niemand der Verantwortung für eigenes Handeln. Wer es anwendet, hat für die richtige Anwendung im konkreten Fall Sorge zu tragen.
- Das DVGW-Regelwerk ist nicht die einzige, sondern eine wichtige Erkenntnisquelle für fachgerechte Lösungen. Es kann nicht alle möglichen Sonderfälle erfassen, in denen weitergehende oder einschränkende Maßnahmen geboten sein können.

ISSN 0176-3490

Preisgruppe: 9

© DVGW, Bonn, März 2017

DVGW Deutscher Verein des Gas- und Wasserfaches e. V.
Technisch-wissenschaftlicher Verein

Josef-Wirmer-Straße 1–3
D-53123 Bonn

Telefon: +49 228 9188-5
Telefax: +49 228 9188-990
E-Mail: info@dvgw.de
Internet: www.dvgw.de

Jede Art der urheberrechtlichen Verwertung und öffentlichen Wiedergabe, auch auszugsweise, nur mit Genehmigung des DVGW Deutscher Verein des Gas- und Wasserfaches e. V., Bonn, gestattet.

Vertrieb: Wirtschafts- und Verlagsgesellschaft Gas und Wasser mbH, Josef-Wirmer-Str. 3, 53123 Bonn
Telefon: +49 228 9191-40 · Telefax: +49 228 9191-499
E-Mail: info@wvgw.de · Internet: www.wvgw.de
Art. Nr.: 309898

Inhalt

Vorwort **5**

Einleitung **7**

1 Anwendungsbereich **10**

2 Begriffe, Symbole, Einheiten und Abkürzungen **10**

3 Bestehende Alternativen **11**
3.1 Initiativen des Gesetzgebers / Regulierungsbehörde 12
3.1.1 IT-Sicherheitsgesetz 12
3.1.1.1 Kurzbeschreibung 12
3.1.1.2 Ziel/Fokus/Geltungsbereich 12
3.1.1.3 Anwendbarkeit 13
3.1.1.4 Implementierungsaufwand 13
3.1.1.5 Berücksichtigte Bedrohung 13
3.1.2 IT-Sicherheitskatalog 14
3.1.2.1 Kurzbeschreibung 14
3.1.2.2 Ziel/Geltungsbereich 14
3.1.2.3 Anwendbarkeit 15
3.1.2.4 Implementierungsaufwand 15
3.1.2.5 Risikobeurteilung 15
3.1.3 Bundesamt für Sicherheit in der Informationstechnik (BSI) – Grundschutz 15
3.1.3.1 Kurzbeschreibung 15
3.1.3.2 Ziel/Fokus/Geltungsbereich 16
3.1.3.3 Anwendbarkeit 16
3.1.3.4 Implementierungsaufwand 16
3.1.3.5 Berücksichtigte Bedrohungen 17
3.1.3.6 Abgedeckte Schutzziele 17
3.2 Normen und Richtlinien 17
3.2.1 DIN ISO/IEC 27000er Reihe 17
3.2.1.1 Kurzbeschreibung 17
3.2.1.2 Ziel/Fokus/Geltungsbereich 18
3.2.1.3 Anwendbarkeit 19
3.2.1.4 Implementierungsaufwand 20
3.2.1.5 Berücksichtigte Bedrohungen 20
3.2.1.6 Abgedeckte Schutzziele 20

3.2.2 IEC 62351 20
3.2.2.1 Kurzbeschreibung 20
3.2.2.2 Ziel/Fokus/Geltungsbereich 21
3.2.2.3 Anwendbarkeit 22
3.2.2.4 Implementierungsaufwand 22
3.2.2.5 Berücksichtigte Bedrohungen 22
3.2.2.6 Abgedeckte Schutzziele 23
3.3 Weitere Dokumente 23
3.3.1 BDEW-Whitepaper 23
3.3.1.1 Kurzbeschreibung 23
3.3.1.2 Ziel/Fokus/Geltungsbereich 23
3.3.1.3 Anwendbarkeit 23
3.3.1.4 Implementierungsaufwand 23
3.3.1.5 Berücksichtigte Bedrohungen 24
3.3.1.6 Abgedeckte Schutzziele 24
3.4 Zusammenfassung 24
3.4.1 Wirksamkeit der bestehenden Regeln 24
3.4.2 Schlussfolgerung und Handlungsempfehlung 24

4 Weiteres Vorgehen für eine ganzheitliche Implementierung im Netzbetrieb 25
4.1 Managementunterstützung 27
4.2 Definition des Anwendungsbereiches 27
4.3 Inventarisierung der Informationswerte 29
4.4 Risikomanagement 31
4.5 Erklärung der Anwendbarkeit und Risikobehandlung 33
4.6 Planen der operativen ISMS-Einführung 33
4.7 ISMS-Einführungsprogramm (Dokumente) 34
4.8 Operatives ISM starten 34
4.9 Operatives ISMS „leben“ 34
4.10 Bewertung der Wirksamkeit des ISMS 35
4.11 Korrekturmaßnahmen 35
4.12 „Probelauf“ für die Zertifizierung 35
4.13 Zertifizierungsaudit 35

5 Meldepflicht 37
5.1 Hintergrund 37
5.2 Kontaktstelle 37
5.3 Anlagenkategorien und Schwellenwerte nach BSI-KritisV (Auszüge) 38
5.4 Unterscheidung der IT-Störungen 39
5.4.1 Gewöhnliche IT-Störung 40
5.4.2 Außergewöhnliche IT-Störung 41
5.5 Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur 41
5.6 Durchführung der Meldung 41
5.7 Schnelligkeit einer Meldung 41

6 Anhang 42
6.1 Anhang: Checkliste für die Vorbereitung eines ISMS im Unternehmen 42
6.2 Anhang: Dokumentation eines ISMS 43
6.3 Anhang: Ermittlung Ist-Situation und Anpassungsbedarf Managementrahmen ISO/IEC 27001:2013 (berücksichtigt nicht die Anforderungen aus Annex A) 45

Vorwort

Die Unterstützung durch Informations- und Kommunikationstechnik (IKT) mit der wachsenden Abhängigkeit von Selbiger geht mit Chancen und Risiken einher. Um die Vorteile moderner IKT sicher nutzen zu können, wird ein angemessener Schutz gegen Bedrohungen auch im Bereich des Netzbetriebs der Strom- und Gasversorgung auf unterschiedlichen Netzebenen bzw. Druckstufen angestrebt.

Neben dem verabschiedeten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) gibt es eine Vielzahl an weiteren Regelungen, Normen und Empfehlungen, deren Ziel es ist, die Informationssicherheit in Energieversorgungsunternehmen zu gewährleisten.[1] Mit dem IT-Sicherheitsgesetz soll Gefährdungen der Informationssicherheit besonders schützenswerter und sogenannter Kritischer Infrastrukturen (KRITIS) wie z. B. Energie- oder Telekommunikationsnetzen wirksam begegnet werden.

Im August 2015 wurde zudem der in § 11 Abs. 1a Energiewirtschaftsgesetz (EnWG) referenzierte IT-Sicherheitskatalog der Bundesnetzagentur (BNetzA) veröffentlicht.

Der vorliegende IT-Sicherheitskatalog enthält Anforderungen an alle Betreiber von Energienetzen zur Gewährleistung eines angemessenen Schutzes gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Netzbetrieb notwendig sind. Parallel dazu werden Normungsaktivitäten und weitere Empfehlungen erarbeitet bzw. aktualisiert, die zunehmend auch dem Thema Netzbetrieb und Netztechnik zuzuordnen sind wie z. B. die DIN ISO/IEC 27000 Normungsreihe und die IEC 62351 Normungsreihe.

Das vorliegende Dokument nimmt eine grundlegende Einordnung der bestehenden Normen und Regelwerke vor, die für den (informationstechnisch) sicheren Netzbetrieb notwendig sind. Darauf aufbauend wurde eine Analyse und ein Ausblick auf den weiteren Handlungsbedarf für die Ausgestaltung einer sicheren Informationstechnik (IT) im Netzbetrieb erarbeitet.

---

1 In diesem Zusammenhang sei erwähnt, dass mit Inkrafttreten des Gesetzes zur Digitalisierung der Energiewende im Jahr 2016 die Grundlage für die flächendeckende Einführung von intelligenten Zählern und Messsystemen gelegt wurde. In dem Gesetz werden gleichfalls hohe technische Standards zur Gewährleistung von Datenschutz und Datensicherheit, bereichsspezifische Datenschutzregeln für die Marktkommunikation sowie Regelungen im Zusammenhang mit dem Einbau von intelligenten Zählern zur Ermöglichung von intelligentem Last- und Erzeugungsmanagement vorgegeben.

Darüber hinaus gibt der FNN-/DVGW-Hinweis weitere Hilfestellungen zur Einführung eines Informationssicherheits-Managementsystems (ISMS), welches gemäß § 11 Abs. 1a EnWG verbindlich einzuführen ist. Der Hinweis richtet sich an Netzbetreiber und Netzserviceunternehmen der Sparten Strom und Gas.

Die vorherige Fassung des FNN-/DVGW-Hinweises (Dezember 2015) wurde aktualisiert und insbesondere um die Meldepflichten von Informationssicherheits-Vorfällen[2] im Zuge der Veröffentlichung des BSI-Gesetzes (BSIG) in Verbindung mit der BSI-Kritisverordnung (BSI KritisV) ergänzt. Die hier dokumentierten Grundlagen sind grundsätzlich für alle Sparten anwendbar.

Fokus dieses Dokuments sind die bestehenden oder absehbar in Kraft tretenden nationalen Normen (inkl. Vornormen), Gesetze und Richtlinien (Stand Dezember 2016). Darüber hinaus existieren weitere Regelwerke, u. a. auf europäischer Ebene (z. B. ENISA), welche nicht Teil der Betrachtungen dieses Dokuments sind.

Dieses Dokument erscheint mit gleichem Wortlaut als FNN-DVGW-Hinweis „Informationssicherheit in der Energieversorgung“ beim Forum Netztechnik/Netzbetrieb im VDE (FNN).

2 Einzuschließen sind auch informationstechnische Störungen, die den sicheren Betrieb beeinträchtigen.