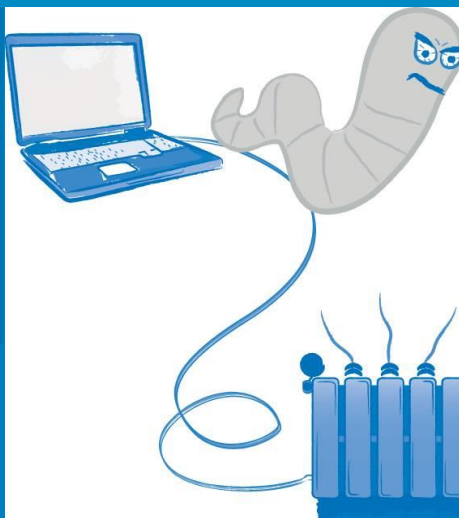


FNN-/DVGW-Hinweis



Informationssicherheit in der Energieversorgung

**Hilfestellung zur Einordnung und
Umsetzung**

Dezember 2016

in Kooperation mit

FNN



VDE



Impressum

© Forum Netztechnik / Netzbetrieb im VDE (FNN)

Bismarckstraße 33, 10625 Berlin

Telefon: + 49 (0) 30 3838687 0

Fax: + 49 (0) 30 3838687 7

E-Mail: fnn@vde.com

Internet: <http://www.vde.com/fnn>

Dezember 2016

Informationssicherheit in der Energieversorgung

Hilfestellung zur Einordnung und Umsetzung

Inhaltsverzeichnis

1	Einleitung	11
1.1	Bedeutung der Informationssicherheit in der Strom- und Gasversorgung	11
1.2	Begriffe und wesentliche informatorische Schutzziele	12
2	Bestehende Initiativen	15
2.1	Initiativen des Gesetzgebers / Regulators.....	15
2.1.1	IT-Sicherheitsgesetz	15
2.1.2	IT-Sicherheitskatalog	17
2.1.3	Bundesamt für Sicherheit in der Informationstechnik (BSI) – Grundsatz	19
2.2	Normen und Richtlinien	20
2.2.1	DIN ISO/IEC 27000er Reihe	20
2.2.2	IEC 62351	24
2.3	Weitere Dokumente	26
2.3.1	BDEW-Whitepaper	26
2.4	Zusammenfassung	27
2.4.1	Wirksamkeit der bestehenden Regeln	27
2.4.2	Schlussfolgerung und Handlungsempfehlung	28
3	Weiteres Vorgehen für eine ganzheitliche Implementierung im Netzbetrieb.....	29
3.1	Managementunterstützung	31
3.2	Definition des Anwendungsbereiches	31
3.3	Inventarisierung der Informationswerte	33
3.4	Risikomanagement (Einschätzung und Behandlung)	35
3.5	Erklärung der Anwendbarkeit und Risikobehandlungsplan.....	37
3.6	Planen der operativen ISMS-Einführung.....	37
3.7	ISMS Einführungsprogramm (Dokumente)	38
3.8	Operatives ISMS starten	38
3.9	Operatives ISMS „leben“	38
3.10	Bewertung der Wirksamkeit des ISMS	39
3.11	Korrekturmaßnahmen.....	39
3.12	„Probelauf“ für die Zertifizierung	39
3.13	Zertifizierungsaudit	40
4	Meldepflicht	42
4.1	Hintergrund	42
4.2	Kontaktstelle	42
4.3	Anlagenkategorien und Schwellenwerte nach BSI-KritisV (Auszüge)	43
4.4	Unterscheidung der IT-Störungen	45
4.4.1	Gewöhnliche IT-Störung	45
4.4.2	Außergewöhnliche IT-Störung	46
4.5	Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur	46
4.6	Durchführung der Meldung	46
4.7	Schnelligkeit einer Meldung.....	47
5	Anhang	48

5.1	Anhang: Checkliste für die Vorbereitung eines ISMS im Unternehmen.....	48
5.2	Anhang: Dokumentation eines ISMS.....	51
5.3	Anhang: Ermittlung Ist-Situation und Anpassungsbedarf Managementrahmen ISO/IEC 27001:2013 (berücksichtigt nicht die Anforderungen aus Annex A)	55