Der Mensch an der Schnittstelle zur Technik: Praxishilfe in der Umsetzung von Datensicherheit durch den IT-Security-Navigator

ISD am 29.09.2017

Dr. Dennis-Kenji Kipker
Dipl.-Ing. Sven Müller

Gefördert vom
FKZ: 16KIS0213
bis 16KIS0216

Bundesministerium für Bildung und Forschung

Universität der Bundeswehr München
FAU Friedrich-Alexander Universität Erlangen-Nürnberg
DKE VDE DIN
Universität Bremen

Ein Fall aus der Praxis:

Sie sind 20 Jahre lang **Wassermeister** in einem kleineren Wasserwerk gewesen. In dieser Funktion waren und sind Sie für die Herstellung qualitativ hochwertigen Trinkwassers zuständig. Infolge des IT-SiG/der BSI-KritisV wird Ihr Arbeitgeber noch knapp in **KRITIS** eingestuft. Er legt Ihnen einen **Änderungsvertrag** für Ihr bestehendes Beschäftigungsverhältnis vor, demzufolge Sie nunmehr (auch) die Funktion des **IT-Sicherheitsbeauftragten** in Ihrem Betrieb wahrnehmen. Angenommen, Sie unterzeichnen das Dokument – **was können Sie nun tun**?

IT-Sicherheitsrecht – ein Dilemma für den juristischen Laien!

Problem Nr. 1: Wie finde ich die richtigen Gesetze?

Deutsche Erkenntnisquellen für die IT-Security Compliance

- Deutsche Erkenntnisquellen für die IT-Security Compliance – Beispiele “von A bis Z”:
  - AktG, § 91
  - AtG, §§ 7 ff., 44b
  - BDSG, §§ 9, 9a, 11, 42a
  - BSIG, §§ 3, 4, 7, 7a, 8a ff.
  - EnWG, §§ 11 ff., 21e, 49
  - GmbHG, § 43
  - KWG, § 25a
  - TKG, §§ 109, 109a
  - TMG, § 13
  - VAG, § 64a
  - WpHG, § 33
  - **… → Keine kodifizierte gesetzliche Regelung der IT-Sicherheit!**
  - **IT-SiG (2015) → Artikelgesetz! → Änderungsgesetz ändert nur Reihe von Fachgesetzen**

EU-Erkenntnisquellen für die IT-Security Compliance

- Europäische Erkenntnisquellen für die IT-Security Compliance – Beispiele “von alt nach neu”:
  - RL 2002/58/EG über elektronische **Kommunikationsnetze** (E-Privacy-RL) und 2009/136/EG (Cookie-RL)
  - RL 2006/32/EG zu **Energieeffizienz** und **Energiedienstleistungen**
  - RL 2008/114/EG über die **Ermittlung und Ausweisung europäischer kritischer Infrastrukturen** und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern
  - RL 2009/72/EG zum **Elektrizitätsbinnenmarkt**
  - RL 2013/40/EU über **Angriffe auf Informationssysteme**
  - RL 2014/53/EU über die Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die Bereitstellung von **Funkanlagen** auf dem Markt (RED)
  - VO (EU) Nr. 910/2014 über **elektronische Identifizierung und Vertrauensdienste** für elektronische Transaktionen im Binnenmarkt (eIDAS VO)
  - **VO (EU) 2016/679** zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, **Art. 5 Abs. 1 lit. f und Art. 32 (EU DS-GVO, anzuwenden ab 25.05.2018)**
  - **EU NIS-RL (2016) + nationales Umsetzungsgesetz (2017)**

Europäische Rechtsakte

- NIS-RL – Rechtsnatur:
  - EU-Richtlinie (RL) ≠ EU-Verordnung (VO)
  - Art. 288 AEUV (Vertrag über die Arbeitsweise der EU):
    - „Die VO hat allgemeine Geltung. Sie ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.“ → Kein nationales Umsetzungsgesetz zur Wirksamkeit notwendig (z.B. EU DS-GVO)
    - „Die RL ist für jeden Mitgliedstaat […] hinsichtlich des zu erreichenden Ziels verbindlich, überlässt jedoch den innerstaatlichen Stellen die Wahl der Form und der Mittel.“ → Nationales Umsetzungsgesetz zur Wirksamkeit notwendig
  - Deutschland: **Nationales Umsetzungsgesetz** ändert Einzelgesetze ab („Gesetz zur Umsetzung der EU RL 2016/1148“)
  - **Mindestharmonisierung:** Deutschland kann auch ein höheres IT-Sicherheitsniveau schaffen, als es die EU NIS-RL vorgibt

Der **europäische Blick** auf die rechtliche Regulierung von **IT-Sicherheit** hat somit vornehmlich (nur) eine **deutsche Perspektive**, indem das EU-Recht deutsche Gesetzgebungsakte initiiert!

Problem Nr. 2: Wie wende ich die gefundenen Gesetze richtig an?

Gesetzesbeispiel IT-Sicherheitsrecht Nr. 1: BSIG

- § 8a BSIG – Sicherheit in der Informationstechnik Kritischer Infrastrukturen:

  (1) Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 **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.

Gesetzesbeispiel IT-Sicherheitsrecht Nr. 2: BDSG

- § 9 BDSG – Technische und organisatorische Maßnahmen:

  Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben **die technischen und organisatorischen Maßnahmen zu treffen**, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz **genannten Anforderungen**, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Gesetzesbeispiel IT-Sicherheitsrecht Nr. 3: GmbHG

- § 43 GmbHG – Haftung der Geschäftsführer:

  (1) Die Geschäftsführer haben in den Angelegenheiten der Gesellschaft **die Sorgfalt eines ordentlichen Geschäftsmannes** anzuwenden.

  (2) Geschäftsführer, welche ihre **Obliegenheiten verletzen, haften** der Gesellschaft solidarisch für den entstandenen Schaden.

IT-Security Compliance als interdisziplinäres Themenfeld

- IT-Security Compliance als interdisziplinäres Themenfeld:
  - **IT-Security-Bezug** bei gesetzlichen Vorschriften **nicht immer klar erkennbar** bzw. Erwartungshorizont **nicht hinreichend konkretisiert**
  - **Unbestimmte Rechtsbegriffe** bzw. **Generalklauseln** führen zu **Schwierigkeiten in der Anwendungspraxis** insb. für KMUs
    - Bezugnahme auf außerhalb des Rechts liegende technische Sachverhalte
    - Noch nicht abgeschlossene Konkretisierung insb. für neue Gesetze, vgl. **“Stand der Technik” gem. IT-SiG (2015)**

Wie kann man unbestimmte Rechtsbegriffe/Generalklauseln konkretisieren und damit Anwendersicherheit im Umgang mit Cyberlaw schaffen?

→ Durch **technische Normen und Standards**!

Unbestimmte Rechtsbegriffe und deren Konkretisierung

- Beispiel: Konkretisierung des **Standes der Technik beispielsweise nach § 8a BSIG** durch das ISMS:
  - Information Security Management System (**ISMS**) nach ISO/IEC 27001 setzt voraus, dass laufend neue Bedrohungslagen erfasst und wirksame und aktuelle Gegenmaßnahmen implementiert werden
  - Dies umfasst auch technisch neue Situationen, die teils im Anwenderkreis angelangt sind (**Stand der Technik** gem. Definition nach Handbuch der Rechtsförmlichkeit des BMJV)
  - Durch **laufende und aktuelle Anpassung (PDCA + BCM)** technischer Systeme wird dafür Sorge getragen, dass deren Stand nicht auf das Niveau der „allgemein anerkannten Regel der Technik“ zurückfällt, Aktualität braucht aber auch nicht Stand von „Wissenschaft und Technik“ zu genügen
  - **Somit wichtig**: Zuordnung einer getroffenen TOV/TOM zu einer Stufe kann sich im Laufe der Zeit ändern, sodass diese ggf. nicht mehr dem gesetzlich geforderten Standard entspricht!

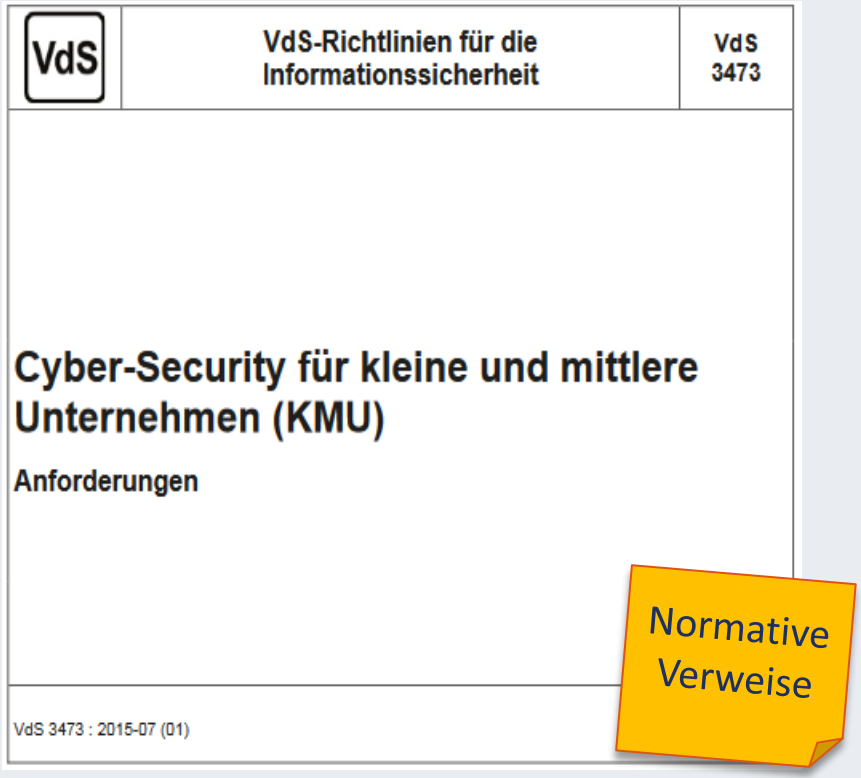
Wer **effektive IT-Security** betreiben will, muss deshalb einen Blick sowohl auf die **Gesetze** wie auch auf die **technischen Normen** werfen!

IT-Grundschutz im Hinblick auf den erforderlichen Aufwand

ISO 270xx Zertifizierung

DIN ISO/IEC 27000 Überblick und Terminologie
DIN EN ISO/IEC 27001 Anforderungen
DIN EN ISO/IEC 27002 Leitfaden für Informationssicherheitsmaßnahmen
DIN SPEC 27003 Unternehmensübergreifende Produktinformationsnetzwerke der Konsumgüterwirtschaft - Terminologie
BS ISO/IEC 27004 Monitoring, measurement, analysis and evaluation
NF Z74-225 NF ISO/CEI 27005 Risikomanagement
BS ISO/IEC 27006 Requirements for bodies providing audit and certification of information security management systems
BS ISO/IEC 27007 Guidelines for information security management systems auditing
PD ISO/IEC TR 27008 Guidelines for auditors on information security controls
DIN ISO/IEC 27009 Sektorspezifische Anwendung der ISO/IEC 27001 - Anforderungen
BS ISO/IEC 27010 Information security management for inter-sector and inter-organizational communications
BS ISO/IEC 27011 Code of practice for information security controls based on ISO/IEC 27002 for telecommunications organizations
BS ISO/IEC 27013 Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
BS ISO/IEC 27014 Governance of information security
DS/ISO/IEC TR 27015 guidelines for financial services
DS/ISO/IEC TR 27016 Organizational economics
DS/ISO/IEC 27017 Code of practice for information security controls based on ISO/IEC 27002 for cloud services
DIN ISO/IEC 27018 Leitfaden zum Schutz personenbezogener Daten (PII) in öffentlichen Cloud-Diensten als Auftragsdatenverarbeitung
DIN ISO/IEC TR 27019 Leitfaden für das Informationssicherheitsmanagement von Steuerungssystemen der Energieversorgung auf Grundlage der ISO/IEC 27002

Cyber-Security für kleine und mittlere Unternehmen (KMU)



Diese Richtlinien enthalten datierte und undatierte Verweise auf andere Regelwerke

BSI-Standard 100-2 IT-Grundschutz-Vorgehensweise
BSI-Standard 100-3 Risikoanalyse
BSI-Standard 100-4 Notfallmanagement

DIN EN 50173 Informationstechnik - Anwendungsneutrale Kommunikationsverkabelung

DIN EN 50174 Informationstechnik - Installation von Kommunikationsverkabelung

DIN EN ISO 9001 Qualitätsmanagementsysteme – Anforderungen

DIN EN ISO 22301 Sicherheit und Schutz des Geheimwesens – Anforderungen

ISO 31000 Risk Management

ISO/IEC 27005 Information technology

VdS 2007 Anlagen der Informationstechnologie

Kontinuierliche Weiterentwicklung der Normen

- **DIN EN ISO/IEC 27038:2016-12** Informationstechnik – Sicherheitsverfahren- **Spezifikation für digitales Schwärzen** Diese Norm legt Methoden für das digitale Schwärzen von digitalen Dokumenten fest. Schwärzen kann auch das Entfernen von Dokument-Metadaten sowie das Entfernen von Informationen, die in das Dokument importiert wurden, umfassen.

- **DIN EN ISO/IEC 27040:2016** Informationstechnik – IT-Sicherheitsverfahren – **Speichersicherheit** liefert Leitlinien für die Speichersicherheit in einer Organisation, in dem sie insbesondere die Anforderungen eines ISMS stützt und empfiehlt den Ansatz des Informationssicherheits-Risikomanagements nach ISO/IEC 27005.

- **Entwurf DIN EN 62443-4-2 (VDE 0802-4-2): 2017-10** Industrielle Kommunikationsnetze – IT-Sicherheit für industrielle Automatisierungssysteme **Teil 4-2: Anforderungen an Komponenten industrieller Automatisierungssysteme** gibt Anforderungen an die IT-Sicherheit von Komponenten an, aus denen ein industrielles Automatisierungssystem aufgebaut ist, insbesondere die eingebetteten Geräte, Netzwerkkomponenten, Host- Komponenten und Softwareanwendungen.

Unsere Praktiker-Lösung zur interdisziplinären Zusammenführung von Recht und Technik – auch für den **Wassermeister** aus dem Eingangsbeispiel – lautet deshalb:

IT-Security Navigator

DKE VDE DIN DIN Universität Bremen **IT-Security NAVIGATOR** ITS KRITIS

Start | IT-Security Standards | IT-Security Laws | Research | Notification

Orientierung durch Normen und Gesetze

DKE VDE DIN DIN Universität Bremen **IT-Security NAVIGATOR** ITS KRITIS

Start | IT-Security Standards | IT-Security Laws | Research | Notification

Letzte Änderungen: 2017-07-12

Alle durchsuchen

ID	Standard Title	Coverage	SDO	Commitee	Standard Number	Publication Date	Chapter	Level of Abstraction	Sector	Referenced IT Security Standards	Component Layer	Communication Layer	Information Layer	Functional Layer	Policy Layer	Target User
	Border Control															
28	Information technology - Security techniques - Random bit generation	I	ISO/IEC	ISO/IEC JTC 1/SC 27	18031	2011-11		4	Cryptography	ISO/IEC 9797-2, ISO/IEC 10116, ISO/IEC 10118-3, ISO/IEC 18032, ISO/IEC 18033-3, ISO/IEC 19790	Nein	Nein	Nein	Ja	Ja	Vendor
29	Information technology - Security techniques - Prime number generation	I	ISO/IEC	ISO/IEC JTC 1/SC 27	18032	2005-01		4	Cryptography	ISO/IEC 18031	Nein	Nein	Nein	Ja	Ja	Vendor
30	Information technology - Security techniques - Methodology for IT security evaluation	I	ISO/IEC	ISO/IEC JTC 1/SC 27	18045	2008-08		4		ISO/IEC 10116, ISO/IEC 10118-2, ISO/IEC 10118-3, ISO/IEC 15946-1, ISO/IEC 18031, ISO/IEC 18032, ISO/IEC 18033-1, ISO/IEC 18033-2, ISO/IEC 18033-3	Nein	Nein	Nein	Nein	Nein	
31	Information technology - Security techniques - Cryptographic algorithms and security mechanisms conformance testing	I	ISO/IEC	ISO/IEC JTC 1/SC 27	18367	2014		4		ISO/IEC 19790, ISO/IEC 24759, ISO/IEC 29128 , ISO/IEC 18031 , ISO/IEC 18032 , ISO/IEC 18033-1/4 (all parts) , ISO/IEC 29192-1/4 (all parts)	Nein	Nein	Nein	Nein	Nein	
32	Information technology - Security techniques - Authenticated encryption	I	ISO/IEC	ISO/IEC JTC 1/SC 27	19772	2009-02		4		"ISO/IEC 9797-1 ISO/IEC 10116 ISO/IEC 18033-3"	Nein	Nein	Nein	Nein	Nein	
	Information technology - Security									"ISO/IEC 9796-2, ISO/IEC 9796-3, ISO/IEC 9797-1, ISO/IEC 9798-2, ISO/IEC 9798-3, ISO/IEC 9798-4, ISO/IEC 9798-5, ISO/IEC 9798-6, ISO/IEC 9797-2, ISO/IEC 10118-2, ISO/IEC 10118-3, ISO/IEC						

IT-Security NAVIGATOR

DKE VDE DIN | DIN | Universität Bremen | ITS KRITIS

Letzte Änderungen: 2017-08-16

Alle durchsuchen

Bezeichnung	Abk./Link	Einzelne rechtliche Vorschriften	Unbestimmte Rechtsbegriffe/ Generalklauseln	Technische Normen & Standards	Relevanz	Gesetzesmaterialien	Rechtspr./Literatur	Sektor	Branche	Ebene	Rechtsakt	Bundesland
Gesetz über den Messstellenbetrieb und die Datenkommunikation in intelligenten Energienetzen (Messstellenbetriebsgesetz)	MsbG	Alle, insbes. §§ 19-28; 52; 53; 61; 73; Anlage zu § 22 II 1	Aufrufen	BASI/TR 03109-2 V1.1 TR-03109-2; BASI/TR 03109-6 V1.0; DVGW G 694; PTB-A 50.8; DIN IEC/TS 62056-6-9 (DIN SPEC 42056-6-9); IEC 61968-9; DIN EN 62056-1-0 (VDE 0418-6-1-0); DIN EN 62056-3-1 (VDE 0418-6-3-1); DIN EN 13757-1; DIN EN 13757-2; DIN EN 13757-3;	1		Aufrufen	Energie	Elektrizität	Bundesrecht	Gesetzlich	

Ihre Mitarbeit und Unterstützung ist gefragt...

Der IT-Security-Navigator wird kein statisches Werkzeug bleiben, sondern sich mit den wachsenden rechtlichen und technischen Innovationen weiterentwickeln. Daher möchten wir **alle Nutzer** bitten, ihre Anmerkungen zum Navigator hinsichtlich

- Erweiterungen, Aktualisierungen
- Fehler
- neuer Gesetze und Standards

zu melden.

Bei Fragen und Anmerkungen für

IT-Normen und Standards
DKE
Sven Müller
Tel.: 069 63 08-395
it-securitystandards@vde.com

IT-Recht
Universität Bremen
Dr. Dennis-Kenji Kipker
Tel.: 0421 218 66049
kipker@uni-bremen.de

Wir danken Ihnen für Ihre Mithilfe!

Koordination VDE|DKE:
Andreas Harner
it-securitystandards@vde.com

Koordination DIN|KITS:
Volker Jacumeit

Dr. Dennis-Kenji Kipker
Wissenschaftlicher Geschäftsführer
IGMR
Universität Bremen
Universitätsallee GW1
28359 Bremen
Tel.: 0421 218 66049
Mail: kipker@uni-bremen.de

Dipl.-Ing. Sven Müller
Projektmanager
VDE Kompetenzzentrum Informationssicherheit
VDE e.V.
Stresemannallee 15
60596 Frankfurt am Main
Tel.: 069 6308 395
Mail: sven.mueller@vde.com

Besuchen Sie unsere Website: www.itskritis.de
Folgen Sie uns auf Twitter: @itskritis

der Bundeswehr Universität München

FAU FRIEDRICH-ALEXANDER UNIVERSITÄT ERLANGEN-NÜRNBERG

DKE VDE DIN

Universität Bremen