Neues vom Stand der Technik

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

München, 23.02.2018

DKE
VDE DIN

Corporate Governance & (IT-Security) Compliance

- IT-(Security)Compliance als interdisziplinäres Themenfeld:
  - **IT-Security-Bezug** bei gesetzlichen Vorschriften **nicht immer klar erkennbar** bzw. Erwartungshorizont **nicht hinreichend konkretisiert**
  - Allgemeine gesellschaftsrechtliche Beobachtungs- und Sorgfaltspflichten beziehen sich aber auch auf die Gewährleistung der IT-Security
  - Zugang über sog. "**unbestimmte Rechtsbegriffe**" oder "**Generalklauseln**"
  - Zweck: Implementierung außerhalb des Rechts stehender Sachverhalte in Gesetze → das Recht als "Einfallstor" für technische Vorgaben → **Flexibilität, Anpassungsfähigkeit und Technikoffenheit**
  - Jedoch: **Teils erhebliche Schwierigkeiten in der Anwendungspraxis, vor allem für KMUs**
  - Bei Bezugnahme auf außerhalb des Rechts liegende Sachverhalte
  - Bei noch nicht abschließender Konkretisierung unbestimmter Rechtsbegriffe, z.B. für neue Gesetze, vgl. "Stand der Technik" gem. IT-SiG (2015)
  - **Ausfüllung der unbestimmten Rechtsbegriffe kann v.a. durch technische Normen & Standards erfolgen**

Unbestimmte Rechtsbegriffe und deren Konkretisierung

- Wie können Normen & Standards gesetzestechnisch einbezogen werden?
  - **Verweisung**
  - **Inkorporation**

Unbestimmte Rechtsbegriffe und deren Konkretisierung

- Die normkonkretisierende gleitende Verweisung:
  - Führt zur gesetzlichen Verwendung **unbestimmter Rechtsbegriffe**
  - **Drei wesentliche Kategorien** von unbestimmten Rechtsbegriffen in der gesetzgeberischen Verwendung:
    - Stand von Wissenschaft und Technik
    - Stand der Technik
    - Allgemein anerkannte Regeln der Technik
  - Konkretisiert durch **BMJV: Handbuch der Rechtsförmlichkeit**

Unbestimmte Rechtsbegriffe und deren Konkretisierung

- Die normkonkretisierende gleitende Verweisung:
  - Führt zur gesetzlichen Verwendung **unbestimmter Rechtsbegriffe**
  - **Drei wesentliche Kategorien** von unbestimmten Rechtsbegriffen in der gesetzgeberischen Verwendung:
    - Stand von Wissenschaft und Technik
    - Stand der Technik
    - Allgemein anerkannte Regeln der Technik
  - Konkretisiert durch **BMJV: Handbuch der Rechtsförmlichkeit**

Unbestimmte Rechtsbegriffe und deren Konkretisierung

Allgemein anerkannte Regeln der Technik

- Schriftlich fixierte oder mündlich überlieferte technische **Festlegungen**
- Für Verfahren, Einrichtungen und Betriebsweisen, die nach **herrschender Auffassung von Fachleuten**, Anwendern, Verbrauchern und der öffentlichen Hand die **Eignung besitzen**,
- das **gesetzlich vorgegebene Ziel** zu erreichen und
- die sich in der Praxis **allgemein bewährt** haben bzw. deren Bewährung in naher Zeit bevorsteht

Stand der Technik

- Entwicklungsstand **fortschrittlicher Verfahren**, Einrichtungen und Betriebsweisen,
- der nach **herrschender Auffassung** führender Fachleute das Erreichen des gesetzlich vorgegebenen **Ziels gesichert** erscheinen lässt, wenn sich
- die entsprechenden Verfahren bereits in der Praxis **bewährt haben** oder zumindest aber im Betrieb mit Erfolg **erprobt wurden**

Stand von Wissenschaft und Technik

- Entwicklungsstand **fortschrittlichster Verfahren**
- Nach Auffassung **führender Fachleute** aus Wissenschaft und Technik
- Auf der Grundlage **neuester wissenschaftlich vertretbarer Erkenntnisse** im Hinblick auf das gesetzgeberische Ziel für erforderlich gehalten
- **Zielerreichung** erscheint gesichert

Unbestimmte Rechtsbegriffe und deren Konkretisierung

- Drei-Stufen-Theorie (BVerfG, Beschluss vom 08.08.1978, 2 BvL 8/77):
  - Ermöglicht bessere **Abgrenzung** zwischen vorgenannten drei unbestimmten Rechtsbegriffen
  - Je weiter eine bestimmte technische Vorgehensweise oder Methode in der Praxis etabliert und allgemein anerkannt ist, umso eher wird von einer **allgemein anerkannten Regel der Technik** auszugehen sein
    - Folglich immer dann einschlägig, wenn eine Maßnahme der **Mehrheitsauffassung** aller Praktiker entspricht
  - Gegensatz dazu: **Stand von Wissenschaft und Technik**
    - Vornehmlich solche Methoden, die nur dem aktuellsten technischen Erkenntnisstand entsprechen und sich folglich in der Praxis **noch nicht durchgesetzt** haben.
  - **Stand der Technik** als Mittelmaß
    - Solche Vorkehrungen, die zwar noch **nicht unbedingt bei jedem Fachmann** oder Anwender angelangt sein müssen, aber zugleich auch nicht so neu sind, dass sie die Grenze des wissenschaftlich bzw. technisch Realisierbaren bedeuten

Normenreihe ISO/IEC 2700x
Sektor-/branchenspezifische Normen

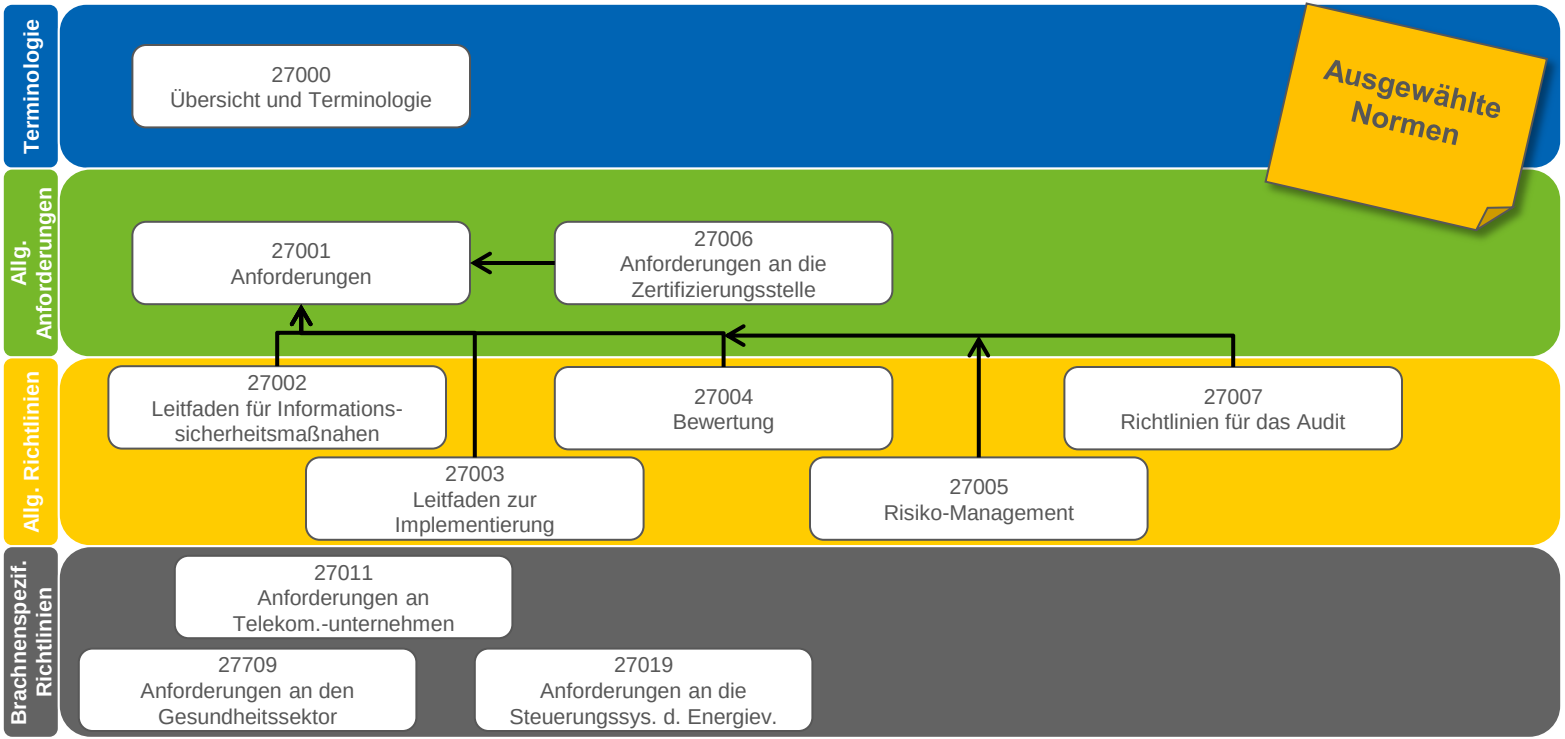
Sektor- bzw. Brachen-Spezifika

- ISO 27010 Informationsaustausch in kritischen Infrastrukturen
- ISO 27017/27018 Cloud Diensten
- ISO 27011 Informationssicherheit Telekommunikations-anbieter
- ISO 27019 Prozesssteuerung Energiesektor
- ISO 27015 Informationssicherheit im Finanzsektor
- ISO 27799 Health sector security

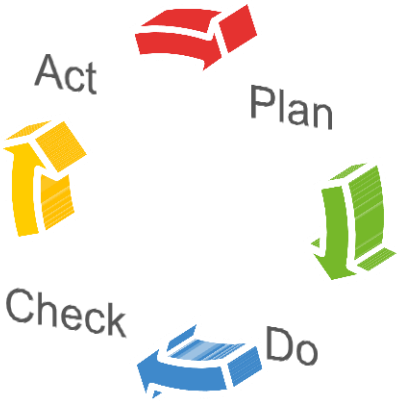
Themenspezifische Standards

- ISO 27031 Geschäftskontinuität
- ISO 27032 Cyber-Sicherheit
- ISO 27033 Netzwerksicherheit
- ISO 27034 Anwendungssicherheit
- ISO 27035 Vorfallmanagement
- ISO 27036 Lieferantensicherheit
- ISO 27037 Sicherung und Erhaltung digitaler Beweismittel
- ISO 27038 Digitales Schwärzen
- ISO 27039 Einruchserkennungs-system
- ISO 27040 Speichersicherheit
- ISO 27041 Vorfall-Untersuchungs-methoden
- ISO 27042 Analyse und Interpretation digitaler Beweise
- ISO 27043 Untersuchung von Vorfällen

ISO/IEC 27001 Informationssicherheit
Aufbau der ISO 2700x-Normenreihe in Anlehnung an ISO 27000



ISO/IEC 27001 Informationssicherheit
PDCA



4. Kontext der Organisation

- 4.1 Verstehen der Organisation und ihres Kontextes
- 4.2 Verstehen der Erfordernisse und Erwartungen interessierter Parteien
- 4.3 Festlegen des Anwendungsbereichs des ISMS
- 4.4 ISMS*

5. Führung

- 5.1 Führung und Verpflichtung
- 5.2 Politik
- 5.3 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation

6.Planung

- 6.1 Maßnahmen zum Umgang mit Risiken und Chancen
- Informationssicherheitsziele und Planung zu deren Erreichung

7.Unterstützung

- 7.1 Ressourcen
- 7.2 Kompetenz
- 7.3 Bewusstsein
- 7.4 Kommunikation
- 7.5 Dokumentierte Information

8. Betrieb

- 8.1 Betriebliche Planung und Steuerung
- 8.2Informationssicherheitsrisikobeurteilung
- 8.3 Informationssicherheitsrisikobehandlung

9. Bewertung der Leistung

- 9.1 Überwachung, Messung, Analyse und Bewertung
- 9.2 internes Audit
- 9.3 Managementbewertung

10. Verbesserung

- 10.1 Nichtkonformität und Korrekturmaßnahmen
- 10.2 Fortlaufende Verbesserung

*ISMS - Informationssicherheitsmanagementsystem

IT-Sicherheit durch Normen und Standards
Zertifizierung nach ISO/IEC 27001

- **Personalsicherheit**

Ziel: Es ist sichergestellt, dass Beschäftigte und Auftragnehmer ihre Verantwortlichkeiten verstehen und für die für sie vorgesehenen Rollen geeignet sind.

Anleitung zur Umsetzung:

a) Vorhandensein zufriedenstellender Leumundszeugnisse, z. B. ein dienstliches und ein persönliches Zeugnis;

b) ein auf Vollständigkeit und Richtigkeit geprüfter Lebenslauf des Bewerbers;

c) Bestätigung angegebener akademischer und beruflicher Qualifikationen;

d) unabhängige Identitätsüberprüfung (Reisepass oder ähnliches Dokument);

e) detailliertere Nachweise, wie Bonitätsprüfung oder Überprüfung des Strafregisters.

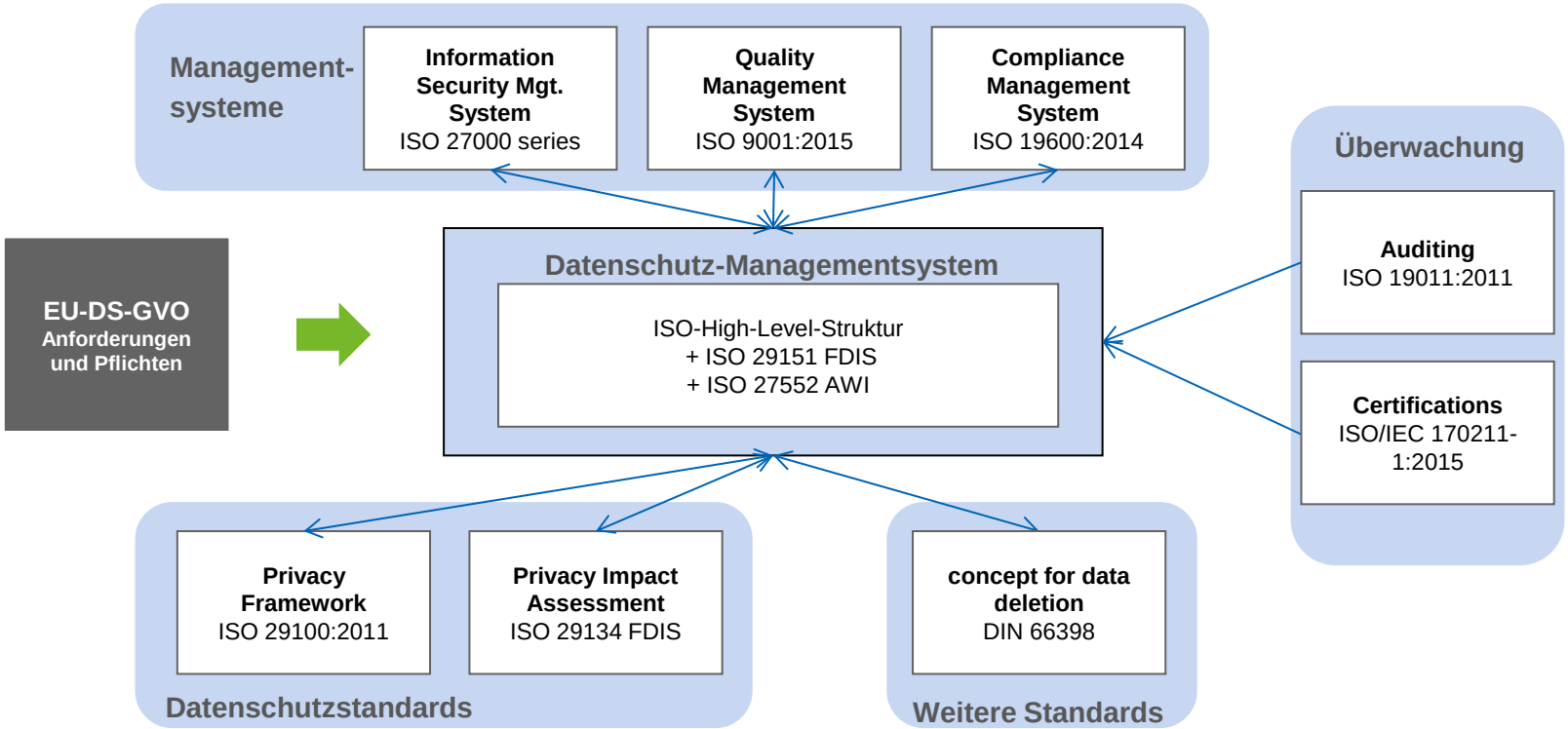
Wenn eine Person für eine bestimmte Rolle der Informationssicherheit angestellt wird, sollten Organisationen sicherstellen, dass der Bewerber:

a) über die notwendige Kompetenz für die Sicherheitsaufgabe verfügt;

b) über die erforderliche Vertrauenswürdigkeit verfügt, insbesondere wenn die Rolle von entscheidender Bedeutung für die Organisation ist.

Quelle: ISO 27002:2017

Informationssicherheit
Normen/Standards/Richtlinien zur Umsetzung der DSGVO



Quelle: Datenschutz-Compliance nach der DS-GVO, Bundesanzeiger Verlag

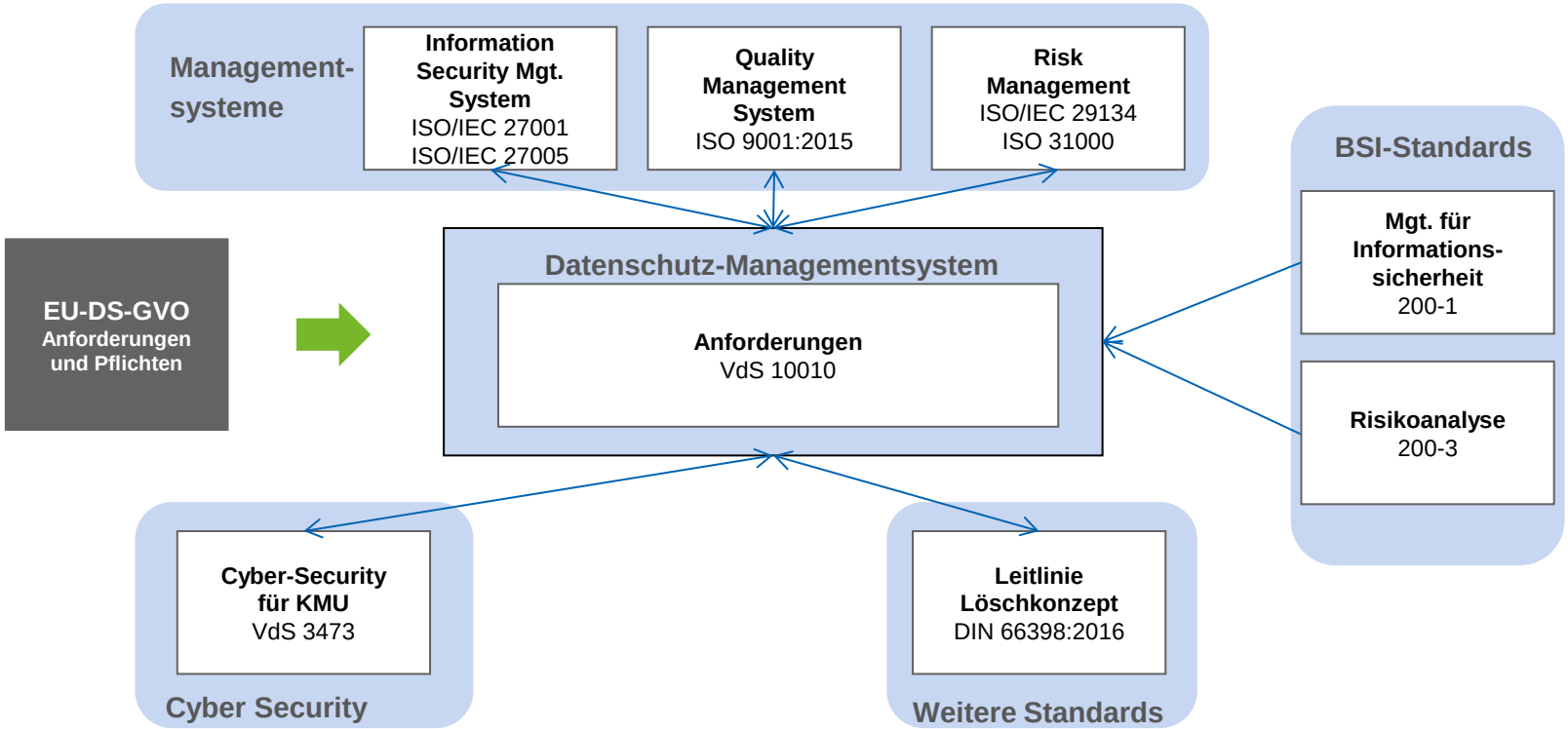
Informationssicherheit
Mögliche Standardlöschfristen eines TK-Dienstleisters

sofort	42 Tage	180 Tage	1 Jahr	4 Jahre*	7 Jahre*	11 Jahre*
TMG		**TKG**		**BGB (3 Jahre)**	**AO, HGB (6 Jahre)**	**AO, HGB (10 Jahre)**
Die Frist „sofort“ ergibt sich aus § 13 Abs. 4Nr.2	Frist frei gewählt		Frist frei gewählt	§ 195 i.V.m. § 199 BGB: 3 Jahre		

* Weil die Jahresfrist nach AO/HGB am Ende des Kalenderjahres beginnt, in dem ein Buch geschlossen wird.

Quelle: DIN 66398:2016-05 Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten

Informationssicherheit
Normen/Standards/Richtlinien zur Umsetzung der DSGVO



Quelle: eigene Darstellung

Zuordnung ISO/IEC 27001 sowie ISO/IEC 27002 und IT-Grundschutz

IT-Grundschutz beschreibt mit Hilfe der BSI-Standards 200-1, 200-2 und 200-3 eine Vorgehensweise zum Aufbau und zur Aufrechterhaltung eines Managementsystems für Informationssicherheit (ISMS).

Die IT-Grundschutz-kataloge beschreiben die Umsetzung der damit einhergehenden Maßnahmenziel und Maßnahmen.

Das damit aufgebaute ISMS erfüllt die Anforderungen der ISO 27001 und verfügt über ein Äquivalent zu den Handlungsempfehlungen der ISO 27002.

Quelle: Zuordnungstabelle ISO 27001 sowie ISO 27002 und IT-Grundschutz

IT-Sicherheit durch Normen und Standards
BSI-Publikationen

BSI-Standards zur Informationssicherheit

Informationssicherheit und IT-Grundschutz

BSI-Standard 200-1
Managementsysteme für Informationssicherheit (ISMS)

BSI-Standard 200-2
IT-Grundschutz-Methodik

BSI-Standard 200-3
Risikoanalyse auf der Basis von IT-Grundschutz

BSI-Standard 100-4
Notfallmanagement

IT-Grundschutz-Kompendium

Kapitel 1 Vorspann
Kapitel 2 Schichtenmodell und Modellierung

Elementare Gefährdungen

Schichten

Prozess-Bausteine:
- ISMS (Sicherheitsmanagement)
- ORP (Organisation & Personal)
- CON (Konzepte & Vorgehensweise)
- OPS (Betrieb)
- DER (Detektion & Reaktion)

System-Bausteine:
- IND (Industrielle IT)
- APP (Anwendungen)
- SYS (IT-Systeme)
- NET (Netzte & Kommunikation)
- INF (Infrastruktur)

IT-Sicherheit durch Normen und Standards
BSI-Standard 200-2

Informationssicherheitsbeauftragte

- Identifikation mit den Zielsetzungen der Informationssicherheit, Überblick über Aufgaben und Ziele der Institution.
- Kooperations- und Teamfähigkeit, aber auch Durchsetzungsvermögen (Kaum eine Aufgabe erfordert so viel Fähigkeit und Geschick im Umgang mit anderen Personen: Die Leitungsebene muss in zentralen Fragen des Sicherheitsprozesses immer wieder eingebunden werden. Entscheidungen müssen eingefordert werden und die Mitarbeiter müssen, eventuell mit Hilfe des Bereichs-Sicherheitsbeauftragten, in den Sicherheitsprozess mit eingebunden werden.)
- Erfahrungen im Projektmanagement, idealerweise im Bereich der Systemanalyse und Kenntnisse über Methoden zur Risikobewertung.
- Grundlegende Kenntnisse über die Prozesse und Fachaufgaben innerhalb der Institution und soweit erforderlich, Grundkenntnisse in den Bereichen IT und ICS.
- Ein Informationssicherheitsbeauftragter muss außerdem die Bereitschaft mitbringen, sich in neue Gebiete einzuarbeiten und Entwicklungen in der IT zu verfolgen. Er sollte sich so aus- und fortbilden, dass er die erforderlichen Fachkenntnisse für die Erledigung seiner Aufgaben besitzt.

IT-Sicherheit durch Normen und Standards
BSI-Standard 200-2

IT-Sicherheitsbeauftragter

Als Aufgaben des IT-Sicherheitsbeauftragten sind festzuhalten:

- • die Vorgaben des ISB umsetzen,
- • die Sicherheitsmaßnahmen gemäß IT-System-Sicherheitsleitlinie oder anderer spezifischer Sicherheitsleitlinien umsetzen,
- • projekt- oder IT-systemspezifische Informationen zusammenfassen und an den ISB weiterleiten,
- • als Ansprechpartner der Mitarbeiter vor Ort dienen,
- • Information über Schulungs- und Sensibilisierungsbedarf von Beschäftigten ermitteln

Folgende Qualifikationen sollten vorhanden sein:

- • detaillierte IT-Kenntnisse, da diese die Gespräche mit Mitarbeitern vor Ort erleichtern und bei der Suche nach Sicherheitsmaßnahmen für die speziellen IT-Systeme von Nutzen sind, sowie
- • Kenntnisse im Projektmanagement, die bei der Organisation von Benutzerbefragungen und der Erstellung von Plänen zur Umsetzung und der Kontrolle von Sicherheitsmaßnahmen hilfreich sind.

IT-Sicherheit durch Normen und Standards
BSI-Standard 200-2

ICS-Informationssicherheitsbeauftragte (ICS-ISB)

Als Aufgaben des ICS-Informationssicherheitsbeauftragten sind festzuhalten:

• die allgemein gültigen Sicherheitsvorgaben der Informationssicherheitsleitlinie und weiterer Richtlinien im Bereich ICS umsetzen,

• gemeinsame Ziele aus dem Bereich der industriellen Steuerung und dem Gesamt-ISMS verfolgen und Projekte aktiv unterstützen

Folgende Qualifikationen sollten beim ICS-ISB vorhanden sein:

• spezielle Kenntnisse zu den Prozessen innerhalb der Institution und der industriellen Steuerung,

• ausreichende IT-Kenntnisse, um Fragen der Mitarbeiter vor Ort, der IT-Experten und weiterer Parteien umfassen beantworten zu können,

• Kenntnisse zu Bedrohungen und Schwachstellen innerhalb der industriellen Steuerung,

• Kenntnisse zu Gefährdungen für die Büro-IT, die innerhalb des ICS-Bereichs eingesetzt wird,

• Kenntnisse zu den Themen Change Management und Notfallmanagement.

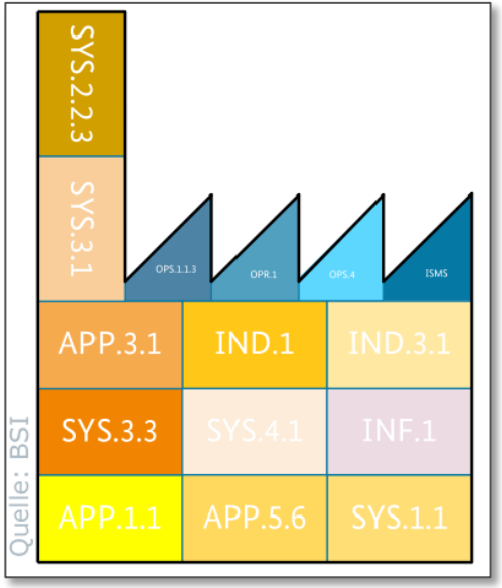
IT-Sicherheit durch Normen und Standards
IT-Grundschutz für KMU

Anwendung der IT-Grundschutz-Profile erfordert,

1. Geringe Security-Fachkenntnis
- Basis: IT-Grundschutz
- Risikoanalyse nur in Ausnahmefällen
- Branchenspezifische Hilfestellung für die Risikoanalyse

2. Wenig Zeitaufwand
- Grundidee der Profile; Anwendern die Modellierung abnehmen
- Gute Passgenauigkeit der Modellierung durch Wahl eine homogenen Geltungsbereichs

3. Wenig bereits vorhandene Dokumentation
- Profil schafft Dokumentation
- Intuitive Anpassung an den Anwender durch Anwendungsfälle



Pilotprofil
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Extern/Diplomarbeiten/Fluchs_Profil_Wasser.html

IT-Sicherheit durch Normen und Standards
IT-Grundschutz für KMU

SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte

Gefährdungslage:

- Unzureichende oder falsche Versorgung mit Verbrauchsgütern
- Unerlaubte Einsicht in ausgedruckte Dokumente
- Fehlerhafter Zugriffsschutz zur Administration
- Missbrauch der Adressbuchfunktion
- Unverschlüsselte Druckerkommunikation
- Fehlende Netztrennung
- Beeinträchtigung von Gesundheit und Umwelt
- Auswertung von Restinformationen
- Yellow Dots

IT-Sicherheit im Handwerk
Grundregeln für ein sicheres „Bring your own device“(BYOD)

- Stellen Sie gut verständliche Sicherheitsrichtlinien auf, aus denen hervorgeht, welche Angestellten mit welchen Geräten auf welche Informationen zugreifen dürfen.
- Stellen Sie sicher, dass Firmendaten nur über verschlüsselte Verbindungen wie WPA2 oder VPN übertragen werden
- Sorgen Sie dafür, dass sensible Daten, wenn überhaupt, nur verschlüsselt auf privaten Mobilgeräten gespeichert werden dürfen.
- Regeln Sie auch, wie und wann Firmendaten, die sich auf privaten Geräten Ihrer Beschäftigten befinden, intern gespeichert werden müssen, zum Beispiel auf einem Firmencomputer.
- Machen Sie auf die Gefahren, die von unseriösen Apps ausgehen können, aufmerksam.
- Setzten Sie ggf. ein „Mobile Device Management“ ein, mit dem Mobilgeräte zentralisiert verwalten können.
- Bluetooth und WLAN sollten nur aktiviert werden dürfen, wenn die Funkverbindungen tatsächlich benötigt werden.
- Erklären Sie die Aktivierung der Kennwortabfrage und automatischen Sperrung bei Nichtgebrauch von mobilen Geräten für verbindlich.

Quelle: http://www.it-sicherheit-in-der-wirtschaft.de/IT-Sicherheit/Navigation/Service/publikationen,did=577944.html

IT-Sicherheit im Bereich Industrie 4.0
Herstellervereinigungen/Behörden

Bundesamt
für Sicherheit in der
Informationstechnik

Bundesamt für Sicherheit in der Informationstechnik (BSI)

- „IT-Grundschutz“
  - Quasi ein Standard für die Erfassung von notwendigen Schutzmaßnahmen und Einführung eines ISMS in Deutschland
  - Kompatibel mit DIN EN ISO/IEC 27001
  - Interaktiver Maßnahmenkatalog speziell für Office-IT

Quelle: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

- „Industrial Control System (ICS) Security“
  - Ist speziell auf Automatisierung bezogen
  - Behandelt die Top 10 Bedrohungen für ICS

Quelle: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_005.pdf?__blob=publicationFile&v=4

IT-Sicherheit im Bereich Industrie 4.0
TOP 10 Bedrohungen für Industrieanlagen 2016 & 2014 (BSI)

Nr. (Nr. alt)	Top 10 (2016)	Top 10 (2014)
1 (3)	Social Engineering und Phishing	Infektion mit Schadsoftware über Internet und Intranet
2 (2)	Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware	Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware
3 (1)	Infektion mit Schadsoftware über Internet und Intranet	Social Engineering
4 (5)	Einbruch über Wartungszugänge	Menschliches Fehlverhalten und Sabotage
5 (4)	Menschliches Fehlverhalten und Sabotage	Einbruch über Wartungszugänge
6 (6)	Internet-verbundene Steuerungskomponenten	Internet-verbundene Steuerungskomponenten
7 (7)	Technisches Fehlverhalten und höhere Gewalt	Technisches Fehlverhalten und höhere Gewalt
8 (9)	Kompromittierung von Extranet und Cloud-Komponenten	Kompromittierung von Smartphones im Produktionsumfeld
9 (10)	(D)DoS Angriffe	Kompromittierung von Extranet und Cloud-Komponenten
10 (8)	Kompromittierung von Smartphones im Produktionsumfeld	(D)DoS Angriffe

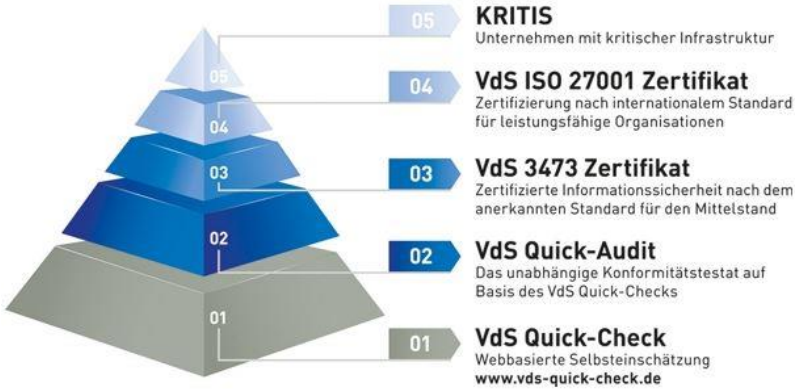
Quelle: Industrial Control System Security – Top 10 Bedrohungen und Gegenmaßnahmen 2016; Version 1.20 vom 01.08.2016 (BSI)

IT-Sicherheit im Bereich Industrie 4.0
Herstellervereinigungen/Behörden

VdS Schadensverhütung GmbH

Cyber-Security für kleine und mittlere Unternehmen (KMU)

- Leichtgewichtige Richtlinie (VdS 3473) speziell für KMU
- Produktionsanlagen werden nicht direkt betrachtet
- Ziel mit möglichst wenig Aufwand einen guten Schutz erreichen
- Inhalt
  - Einführung eines ISMS
  - Konkrete organisatorische und technische Schutzmaßnahmen zu verschiedenen Bereichen von IT-Infrastrukturen
- Weitere Informationen
  - Richtlinie speziell für ICS wird aktuell entwickelt
  - Online-Kurzchecks für Unternehmensseite und Produktionsanlagen unter



IT-Sicherheit im Bereich Industrie 4.0
Normen / Standards / Richtlinien

Verein Deutscher Ingenieure

- „Informationssicherheit in der industriellen Automatisierung Allgemeines Vorgehensmodell“
- Beschreibt Vorgehensmodell für die Etablierung von IT-Sicherheitsmaßnahmen in Automatisierungsanlagen
- Ausrichtung auf Anlage nicht auf organisatorische Maßnahmen
- Adressiert Hersteller, Maschinenbauer/Integratoren, Betreiber
- Letzte Version von 2011 VDI/VDE 2182 Blatt 1
- Letzte Version von 2013 VDI/VDE 2182 Blatt 2.1; 2.2; 3.1; 3.2 & 3.3
- Letzte Version von 2017 VDI/VDE 2182 Blatt 2.3
- aktuelle Projekte VDI/VDE 2182 Blatt 1 und Blatt 4

Quelle: https://www.vdi.de/2182

Normen im Bereich Industrie 4.0
Informationssicherheit in der industriellen Automatisierung

VDI/VDE 2182

- Blatt 1 - Allgemeines Vorgehensmodell (Ausgabedatum 2011-01; aktuelles Projekt)
- Blatt 2.1 - Anwendungsbeispiel des Vorgehensmodells in der Fabrikautomation für Hersteller - Speicherprogrammierbare Steuerung (SPS) (Ausgabedatum 2013-02)
- Blatt 2.2 - Anwendungsbeispiel des Vorgehensmodells in der Fabrikautomation für Maschinen- und Anlagenbauer - Umformpresse (Ausgabedatum 2013-03)
- Blatt 2.3 - Anwendungsbeispiel des Vorgehensmodells in der Fabrikautomation für Betreiber - Presswerk (Ausgabedatum 2017-09)
- Blatt 3.1 - Anwendungsbeispiel des Vorgehensmodells in der Prozessautomation für Hersteller - Prozessleitsystem einer LDPE-Anlage (Ausgabedatum 2013-09)
- Blatt 3.2 - Anwendungsbeispiel des Vorgehensmodells in der Prozessautomation für Integratoren - LDPE-Reaktor (Ausgabedatum 2013-05)
- Blatt 3.3 - Anwendungsbeispiel des Vorgehensmodells in der Prozessautomation für Betreiber - LDPE-Anlage (Ausgabedatum 2013-06)
- Blatt 4 – Empfehlungen zur Umsetzung von Security-Eigenschaften für Komponenten, Systeme und Anlagen (aktuelles Projekt)

IT-Sicherheit im Bereich Industrie 4.0
Herstellervereinigungen/Behörden

PROFIBUS und PROFINET International

- „PROFINET Security Guideline“
- Letzte Version von 2015
- Generelle Einführung in Netzwerksicherheit für Produktionssicherheit

Quelle: https://www.profibus.com/download/profinet-security-guideline/

Open DeviceNet Vendors Association

- „Securing EtherNet/IP Networks“
- Letzte Version von 2011
- Ähnliche Inhalte wie PROFINET Security Guideline
- Zusätzlich wird ein Ausblick auf zukünftige IT-Sicherheitsmaßnahmen gegeben

Quelle: https://www.odva.org/Portals/0/Library/Publications_Numbered/PUB00269R1.1_ODVA_Securing_EtherNetIP_Networks.pdf

IT-Sicherheit im Bereich Industrie 4.0
Herstellervereinigungen/Behörden

Verband Deutscher Maschinen- und Anlagenbau

- „Leitfaden Industrie 4.0 Security“
- Handlungsempfehlung für den Mittelstand
- Beschreibung wie „Industrial Security“ im Kontext von Industrie 4.0 umgesetzt werden muss
- Betrachtung der IT-Sicherheit von Anlagen, Komponenten und Maschinen über deren gesamten Lebenszyklus
- Forderung von „Security by Design“
- Fokus auf Hersteller, Integratoren und Betreiber mit Blickwinkel der Maschinen- und Anlagenbauer
- Vorschläge für konkrete Handlungsempfehlungen in verschiedenen Themenfeldern

Quelle: http://www.vdmashop.de/refs/Leitf_I40_Security_Dt_LR_neu.pdf

IT-Sicherheit im Bereich Industrie 4.0
Automatisierungsstrukturen werden sich künftig ändern

Sicherheit:

„Die Betriebs- und Angriffssicherheit sind in den intelligenten Produktionssystemen erfolgskritische Faktoren. Zum einen sollen von den Produktionsanlagen und Produkten keine Gefahren für Menschen und Umgebung ausgehen; zum anderen müssen die Anlagen und Produkte selbst vor Missbrauch und unbefugtem Zugriff geschützt werden – insbesondere die darin enthaltenen Daten und Informationen. Dazu sind zum Beispiel integrierte Sicherheitsarchitekturen und eindeutige Identitätsnachweise zu verwirklichen, aber auch Aus- und Weiterbildungsinhalte entsprechend zu ergänzen.“

Quelle: https://www.bmbf.de/files/Umsetzungsempfehlungen_Industrie4_0.pdf

Normen im Bereich Industrie 4.0
Light And Right Security (LARS)

- Entwickelt durch BSI und Sirrix AG
  - in Zusammenarbeit mit der TÜV SÜD Rail GmbH
- Frei verfügbar und Open Source
- Einstieg in die Cyber-Sicherheit für KMU
  - Reine Offline-Analyse
- Fragengeleitete Selbsteinschätzung des aktuellen Stands der Cyber-Security
  - Kritikalität von Schwachstellen und der erreichte Security Lever werden automatisch ermittelt
- Empfehlungen zu Schutzmaßnahmen auf Basis beantworteter Fragen
- Schutzmaßnahmen sind entsprechend IT-Grundschutz, ISO/IEC 27001, IEC 62443 und BSI-Security Kompendium zugeordnet
- Wird kontinuierlich überarbeitet

Quelle: https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/Tools/LarsICS/LarsICS_node.html

Normen im Bereich Industrie 4.0
Cyber Security Evaluation Tool (CSET)

- Entwickelt durch ICS-CERT
- Aktuelle Version 8.0 wird als CD-Image (ISO) geliefert
- Umfassender als LARS (Light And Right Security)
  - Ebenfalls reine Offline-Analyse
- Modellierung aller Betrachtungsgegenstände aus Netzwerksicht inkl. Beteiligter Entitäten
  - Inklusive Angabe von Schutzbedarfen bzw. Kritikalität
- Zusätzlich Beantwortung von umfassenden Fragenkatalog
  - Darauf basierend Ermittlung der Gefährdungslage
- Schutzmaßnahmen werden aus einer Datenbank ermittelt
- Gegenüberstellung des eigenen Schutzkonzeptes zu verschiedenen Standards (ausgerichtet auf U.S.A.)

Quelle: https://ics-cert.us-cert.gov/Downloading-and-Installing-CSET

Industrie und Kritische Infrastrukturen
Open Vulnerability Assessment System (OpenVAS)

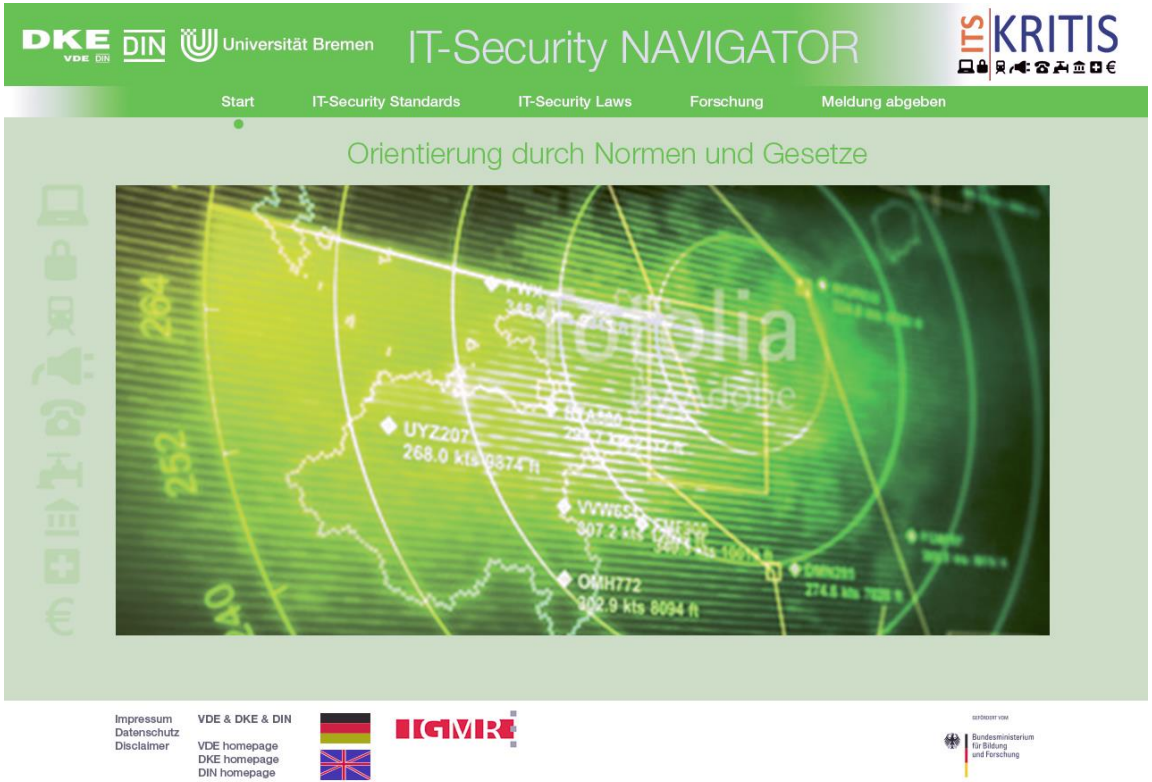
- OpenVAS ist eine Freie Software
- Letzte Version (OpenVAS-9) am 08.03.2017 veröffentlicht
- DFN-CERT steuert seine Sicherheitsmeldungen dem OpenVAS Security Feed bei.
- Das BSI unterstützt verschiedene Funktionen des OpenVas Frameworks sowie viele Schwachstellen-Prüfroutinen
- Das Framework ist ein Teil von Greenbone Networks kommerzieller Schwachstellen-Management-Lösung
- Eine umfangreiche und mächtige Lösung für Schwachstellen-Scanning und Schwachstellen-Management
- Jeden Tag fliessen Verbesserungen und Neuerungen in das Framework (z.B. Penetrations-Tester, Power-User, Forschung und Lehre zu IT-Sicherheit)

Quelle: https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/Tools/OpenVAS/OpenVAS_node.html

Industrie und Kritische Infrastrukturen
Spyware

- Nach einer Studie der Universität von Washington
  - hierbei wurden um die 18 Mio. URLs untersucht -> bei fast 6% davon wurde Spyware gefunden
  - die größten Infektionsraten fanden sich auf Websites mit pornografischem Inhalt, auf Promi-Websites oder Websites zum Herunterladen von Bildschirmhintergründen
  - nicht untersucht wurden Reise- oder Immobilien-Websites
  - nach einer Studie von AOL/NCSA, die dort zitiert wird, waren 80% der getesteten privaten PCs von Spyware befallen
    - mit durchschnittlich 93 einzelnen Spyware-Programmen pro Computer

IT-Security Navigator



https://www.itsecuritynavigator.de

IT-Security Navigator

Anwendung des IT-Security Navigators am Beispiel:
Gesetz über den Messstellenbetrieb und die Datenkommunikation in intelligenten Energienetzen“

DKE VDE DIN Universität Bremen IT-Security NAVIGATOR ITS KRITIS

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

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	
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	DIN EN 1776; DIN EN 16314; DIN CEN/TR 16061 (DIN SPEC 91193); DIN EN 13757-1; DIN EN 13757-2; DIN EN 13757-3; DIN EN 13757-4; DIN EN 13757-5; DIN EN 13757-6	1		Aufrufen	Energie	Gas	Bundesrecht	Gesetzlich	
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	DIN EN 13757-1; DIN EN 13757-2; DIN EN 13757-3; DIN EN 13757-4; DIN EN 13757-5; DIN EN 13757-6;	1		Aufrufen	Energie	Mineralöl	Bundesrecht	Gesetzlich	

DKE VDE DIN | DIN | Universität Bremen

IT-Security NAVIGATOR

ITS KRITIS

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

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

Vielen Dank für Ihre Aufmerksamkeit!

Wir gestalten die e-diale Zukunft.
Machen Sie mit.

Ihr Ansprechpartner:

Sven Müller

Core Safety & Information Technologies
Phone: +49 69 6308 395
sven.mueller@vde.com