BSI-Kritisverordnung
Was kommt auf die Windbranche zu?

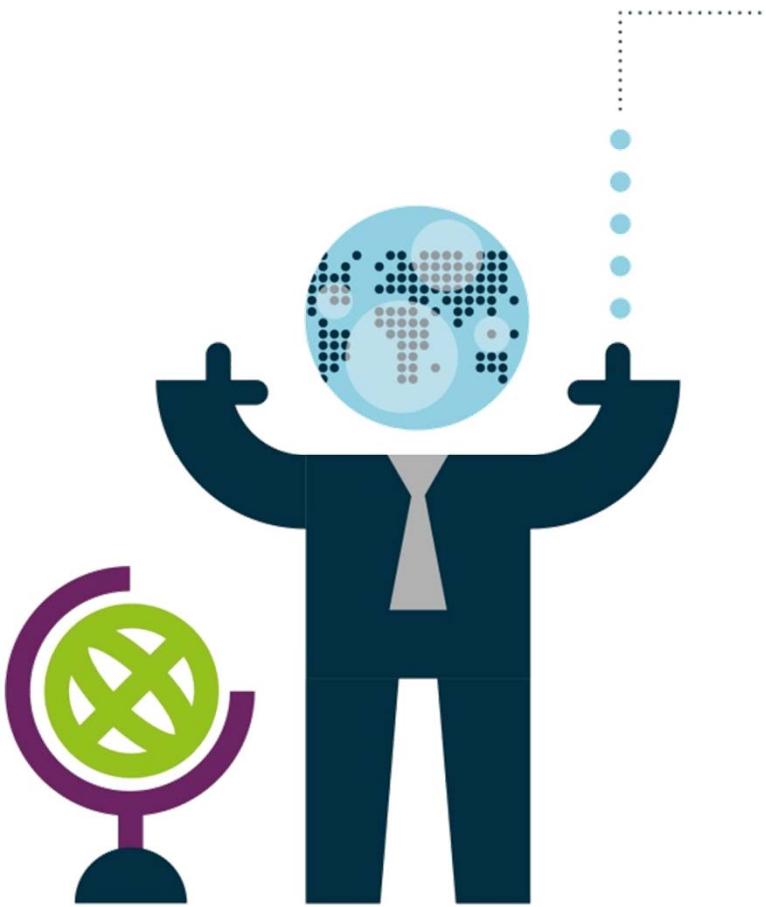
24. Windenergietage
Update April 2016

Dr. Daniel Breuer
12. November 2015
Linstow

Inhaltsverzeichnis

Energy & Utilities bei Osborne Clarke

Osborne Clarke Deutschland



Standorte

- Berlin, Hamburg, Köln, München

Mitarbeiter

- 230 Mitarbeiter insgesamt
- davon 129 Rechtsanwälte und Steuerberater
- davon 47 Partner

Praxisgruppen

- Capital Markets / Banking
- Commercial / Competition
- Corporate
- Employment
- IP
- IT
- Property
- Öffentliches Wirtschafts- und Vergaberecht
- Tax

Branchenfokus

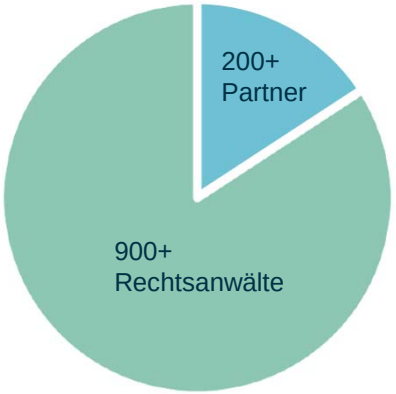
- Digital Business
- Energy & Utilities
- Financial Services
- Life Sciences & Healthcare
- Real Estate & Infrastructure
- Retail
- Transport & Automotive

Osborne Clarke International

mehr als

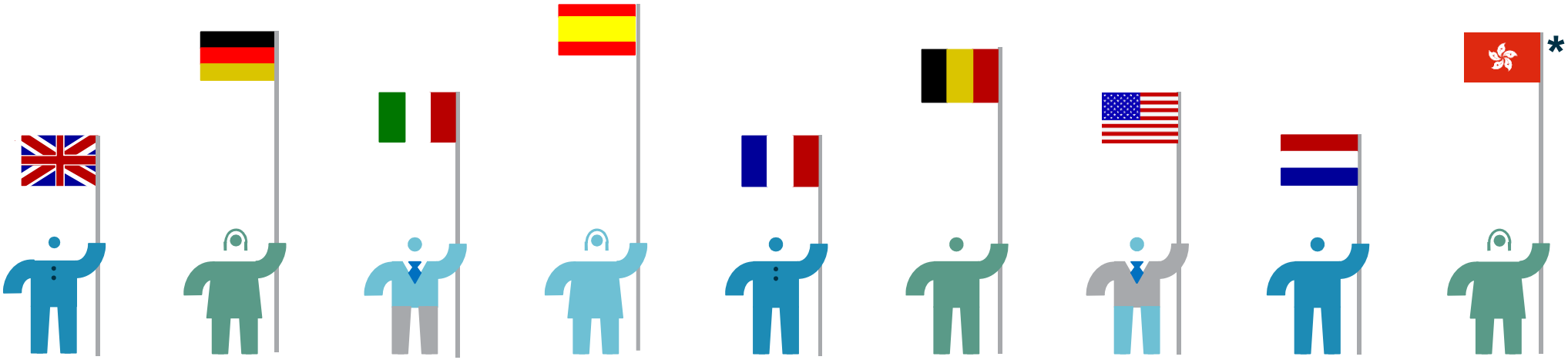
1.300

Mitarbeiter



9 Länder

Belgien: Brüssel
Deutschland: Berlin, Hamburg, Köln, München
Frankreich: Paris
Hongkong*
Italien: Brescia, Mailand, Padua, Rom
Niederlande: Amsterdam
Spanien: Barcelona, Madrid
UK: Bristol, London, Thames Valley
USA: New York, San Francisco, Silicon Valley



* Osborne Clarke unterhält eine strategische Allianz mit Koh Vass & Co.

Unsere Leistungen in der laufenden Rechtsberatung im Sektor Energy & Utilities

Wir unterstützen Sie in allen relevanten Rechtsbereichen:

Energierecht

- Regulierung
- Netzanschluss und -nutzung
- (Regionale) EEG-Direktvermarktung
- Regelenergie-märkte
- Projektverträge, O&M, EPC
- Repowering
- Eigen- und Direktverbrauch
- KAGB-/ZAG-Strukturierung

Gesellschafts-recht / Finan-zierung

- Mergers & Acquisitions
- Joint Ventures, Kooperationen
- Restrukturierung
- Kapitalanlage-recht und Fonds
- Finanzaufsichts-recht
- Projektfinanzierung
- Gesellschafts-gründungen; allg. Gesellschaftsrecht

Öffentliches Recht

- Umwelt- und Planungsrecht
- Baurecht
- Immissionsschutz-recht
- Genehmigungs-verfahren
- Widerspruchs- und Klageverfahren

Prozess-führung

- Komplexe Zivilprozesse
- Schiedsverfahren/ Investitionsschieds -gerichtsbarkeit
- Alternative Dispute Resolution
- Insolvenzverfahren
- Gewährleistungs- und Garantiean-sprüche
- Bes. Missbrauchs-verfahren EnWG
- Clearingstelle EEG

Kartell- und Vergaberecht

- Fusionskontrolle
- Compliance-Beratung
- Vertriebskartell-recht
- Begleitung bei Ausschreibung und Vergabe
- Vergabenachprü-fungsverfahren
- Konzessions-verfahren/Rekom-munalisierung

Handel und Vertrieb

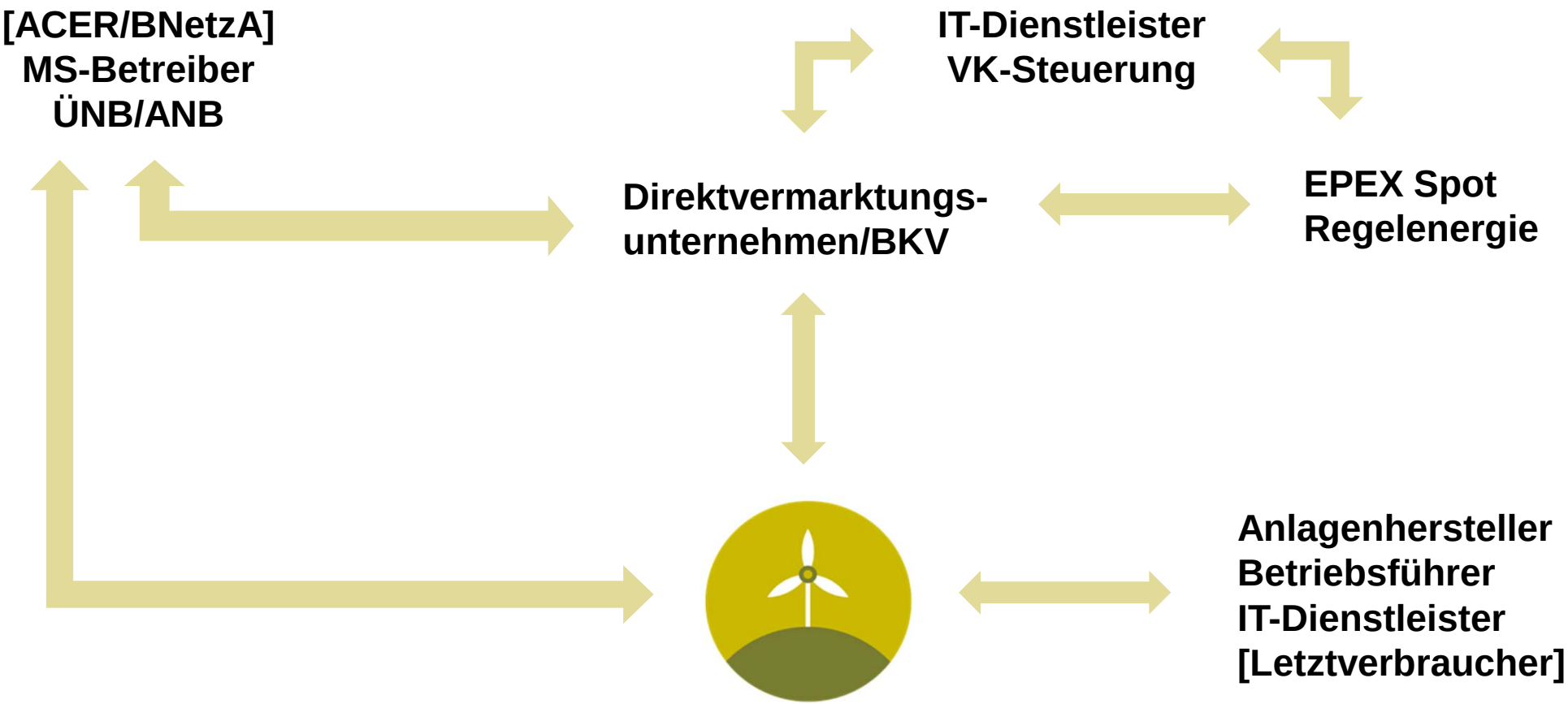
- Brennstoff- und Energiebezugs- und -lieferverträge
- Energie- und Zertifikatehandel
- Preisanpassungs-verhandlungen und -verfahren
- Handels- und Kooperations-verträge
- Vertriebssysteme
- Absatz- und Ver-triebsoptimierung

IT-Recht

- IT-Sicherheit / KRITIS
- IT-Outsourcing
- Datenschutz
- Lizenzverträge
- Forschungs- & Entwicklungs-verträge
- IT-Projektverträge
- Entwicklung und Strukturierung von Smart Grid Produkten und Geschäftsmodellen

Anforderungen an die IT-Sicherheit in der Windbranche

(Kritische) Schnittstellen Informationssicherheit am Beispiel einer Windenergieanlage



IT-Sicherheitsrelevante Schnittstellen und Prozesse

VK-Integration / Handel	WEA-Integration in VK des DVU / IT-Dienstleisters für Handel, Einsatzplanung und -optimierung, Fernsteuerung
Einspeisemanagement	§ 14 EEG: Automatisierte Abregelung durch ANB über Einrichtung zur ferngesteuerten Reduzierung nach § 9 EEG
Fernsteuerung	§ 36 EEG: Ist-Einspeisung (am Netzverknüpfungspunkt) durch Dritten jederzeit abrufen und (über Messsystem) ferngesteuert reduzieren
Monitoring	Fernüberwachung durch Anlagenhersteller, technische Betriebsführer und Prognosedienstleister, Plattformintegration, App-Dienste
Regelenergiemärkte	Autarke Fernwirktechnik; Integration in virtuelles Kraftwerk; weitere Schnittstellen und Dienstleister (neben Betriebsführer und Hersteller)
Messwesen/Datenschutz	Liberalisierter Messstellenbetrieb, Wechselprozesse (WiM); Messstellenbetriebsgesetz; § 9 BDSG (toM); EU-DatenschutzV
Marktkommunikation	Bilanzkreisabrechnung (MaBiS); Marktprozesse Einspeisestellen (BK6-14-110); GPKE; REMIT Meldepflichten als Marktteilnehmer

BSI Lagebericht IT-Sicherheit November 2015

Ursachen	2015
Cloud Computing	>
Software Schwachstellen	^
Hardware Schwachstellen	>
Nutzer-/Herstellerverhalten	^
Kryptografie	>
Internet-Protokolle	^
Mobilkommunikation	^
Sicherheit von Apps	^
Sicherheit von Industriellen Steueranlagen	^

Angriffsmethoden/-mittel	2015
Schadsoftware	^
Social Engineering	>
Gezielte Angriffe – APT (Advanced Persistent Threat)	^
Spam	^
Botnetze	^
DDoS-Angriffe (Distributed Denial of Service)	>
Drive-by-Exploits/Exploit-Kits	^
Identity Theft	^

IT-Sicherheitsgesetz vom 17. Juli 2015

Ziele des IT-Sicherheitsgesetzes

Ziele:

- Verbesserung der Sicherheit informationstechnischer Systeme **Kritischer Infrastrukturen** in Deutschland
- besserer Schutz der Bürger im Internet
- Stärkung des Bundesamts für Sicherheit in der Informationstechnik (BSI) und des Bundeskriminalamtes (BKA)

Schutzzweck:

- Sicherung von Gemeinwohlinteressen im Bereich der Daseinsvorsorge, Vorgabe für entsprechende Betreiberpflichten privater Unternehmen
- Vermeidung erheblicher Störungen der **Verfügbarkeit**, **Integrität**, **Authentizität** und **Vertraulichkeit** der informationstechnischen Systeme, Komponenten und Prozesse

"Artikelgesetz": Änderung bestehender Gesetze (insbesondere **BSI-Gesetz**, Telemedien- und Telekommunikationsgesetz, **Energiewirtschaftsgesetz**)

Adressaten des IT-Sicherheitsgesetzes

Kritische Infrastrukturen i.S.d. § 2 Abs. 10 BSIG

- Einrichtungen, Anlagen oder Teile davon aus den Sektoren Energie u.a., die von **hoher Bedeutung für das Funktionieren des Gemeinwesens** sind
- Kritik: Anwendungsbereich unklar
  - Hohes Maß **unbestimmter Rechtsbegriffe** begründet Rechtsunsicherheit: "Stand der Technik", "angemessener Schutz", "für sicheren Betrieb notwendig", "Mindestvorgaben"
  - Bestimmung Kritischer Infrastrukturen und Kritischer Dienstleistungen ausschließlich durch **BSI-Kritisverordnung** des BMI

Einschränkung des Adressatenkreises durch § 8c BSIG

- § 8c Abs. 1 BSIG: Keine Anwendung der §§ 8a und b BSIG auf Kleinstunternehmen (Jahresumsatz/-bilanz < 2 Mio. € und < 10 Mitarbeiter)
- § 8c Abs. 2 und 3 BSIG: Vorrang branchenspezifischer Spezialregelungen in EnWG

Pflichten der Betreiber Kritischer Infrastrukturen Überblick: BSIG und EnWG (neu) (1)

BSIG	EnWG
§ 8a Abs. 1 Pflicht zur Ergreifung angemessener Vorkehrungen zur Vermeidung von Störungen Berücksichtigung des Stands der Technik; bei kritischen Prozessen ggf. Abschottung erforderlich	**§ 11 Abs. 1b (Betreiber von Energieanlagen)** Pflicht, binnen **zwei Jahren nach Inkrafttreten der VO** einen **angemessenen Schutz** gegen Bedrohungen für TK- und elektronische Datenverarbeitungssysteme zu gewährleisten, die **für einen sicheren Anlagenbetrieb notwendig** sind (sofern als KRITIS bestimmt und an Netz angeschlossen) ➢ Angemessenheit und Notwendigkeit eröffnen weiten Gestaltungsspielraum und Rechtsunsicherheit
§ 8a Abs. 2 Möglichkeit des Vorschlags branchenspezifischer Sicherheitsstandards, wo es fachlich sinnvoll ist. BSI stellt auf Antrag fest, ob diese den Anforderungen des Abs. 1 genügen **§ 11 Abs. 1a (Betreiber von Energieversorgungsnetzen)** Anpassung auf Systeme, die "für einen sicheren Netzbetrieb notwendig" sind sowie Aufhebung der Vermutungsregelung	**§ 11 Abs. 1b (Betreiber von Energieanlagen)** BNetzA erstellt **IT-Sicherheitskatalog** im Benehmen mit dem BSI, jedoch rechtzeitig zum Inkrafttreten? ➢ Sicherheitskatalog zu § 11 Abs. 1a als Blaupause ➢ Angemessener Schutz **liegt vor**, wenn Katalogvorgaben eingehalten und dokumentiert; von Behörde überprüfbar ➢ Im Einzelfall dennoch höhere Anforderungen denkbar?

Pflichten der Betreiber Kritischer Infrastrukturen Überblick: BSIG und EnWG (neu) (2)

BSIG	EnWG
§ 8a Abs. 3 Pflicht zum Nachweis der Erfüllung der Sicherheitsanforderungen mind. alle zwei Jahre durch *Audits, Prüfungen* oder *Zertifizierungen*	**IT-Sicherheitskatalog (bestehender Entwurf - § 11 Abs. 1a)** Verpflichtung des Netzbetreibers die Konformität seines ISMS mit den Anforderungen der DIN ISO/IEC 27001 durch ein *Zertifikat* zu belegen; Audits als reine Sicherheitskatalogmaßnahme (nicht in EnWG)
§ 8b Abs. 3, 4 Zweistufige Meldepflicht gegenüber BSI über **Kontaktstelle**, die binnen **sechs Monaten** ab Inkrafttreten der Rechtsverordnung einzurichten ist: • erhebliche Störungen, die zu einem Systemausfall führen: Namensnennung (personalisierte Meldung) • nur potentielle Beeinträchtigungen, die zu Störung führen können: keine Namensnennung (pseudonyme/anonyme Meldung) ➢ Achtung: Einrichtung Kontaktstelle nicht in EnWG geregelt und § 8b Abs. 3 wg. Vorrang EnWG nicht anwendbar	**§ 11 Abs. 1c** **Zweistufige Meldepflicht** ohne Übergang von sechs Monaten und ohne Pflicht zur Einrichtung zentraler Kontaktstelle, d.h. ➢ **Unverzügliche** Meldung von erheblichen Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten, Prozesse • 1. bei reiner **Bedrohungslage** genügt **anonyme Meldung** • 2. bei **Ausfall** bzw. **Beeinträchtigung** der Funktionsfähigkeit der Kritis-Systeme **personalisierte Meldung** erforderlich BSI dient als zentrale Meldestelle (vgl. § 8b Abs. 1, 2 BSIG) ➢ **GÜA** (SPOC) für anonyme Meldung, obwohl § 8b Abs. 5 nicht anwendbar?

BSI-Kritisverordnung nach § 10 Abs. 1 BSI-Gesetz
Kabinettsbeschluss vom 13. April 2016

Kabinettsbeschluss vom 13. April 2016

Fahrplan des BMI

- Erarbeitung des Referentenentwurfs vom 13. Januar 2016 mit UP KRITIS
- Verbändekonsultation seit Februar 2016
- Anhörung beim BMI am 2. März 2016
- Inkrafttreten der BSI-Kritisverordnung aktuell **Anfang Mai 2016** (am Tag nach Verkündung im BGBl; statt ursprünglich 1. April 2016) für Sektoren Energie, Wasser, IKT und Ernährung
  - (P) Falls Vorlage IT-Sicherheitskatalog für Energieanlagen durch BNetzA verzögert, Unklarheit hinsichtlich Umsetzungsfrist ab Inkrafttreten BSI-KritisV
  - Übergangsregelung jeweils zum 1. April des Folgejahres nach Erreichen der Schwellenwerte in Anlage 1 Teil 1 Nr. 1

Kritische Dienstleistungen im Sektor Energie umfassen **Versorgung** mit:

- **Strom** / Gas / Fernwärme / Kraftstoff und Heizöl

Prozesse und Kenngrößen "Stromversorgung"

Stromerzeugung

- **Erzeugungsanlagen**
- **Dezentrale Erzeugungs-anlagen**
- **Speicheranlagen**
- **Anlagen/Systeme zur Bündelung elektrischer Leistung**
  - Regelbeispiel Pool eines DVU i.S.v. § 5 Nr. 10 EEG
  - vormals "Virtuelle Kraftwerke" bzw. "Anlagen von Poolanbietern"
  - derzeit auch Regelpools erfasst

Stromübertragung

- **Übertragungsnetze**
- **Zentrale Anlagen und Systeme für den Stromhandel**
  - Begrenzung auf EPEX Spotmarkt (Paris) und nicht EEX (Leipzig)

Stromverteilung

- **Verteilernetze**
- **Messstellen**
  - Abgleich mit Regelungen des Messstellenbetriebsgesetzes
  - Einrichtung zur Messung elektrischer Energie mit Möglichkeit zur Ab- und Auslesung der Daten an Übergabepunkten zu Verbrauchern und dezentralen Erzeugungsanlagen

Begriffsbestimmung "Anlagen und Systeme zur Bündelung elektrischer Leistung"

"Anlagen und Systeme zur **Bündelung elektrischer Leistung**, die sowohl von Erzeugungsanlagen als auch Verbrauchseinrichtungen bereitgestellt werden kann; hierzu sind **insbesondere** Direktvermarktungsunternehmen im Sinne von § 5 Nr. 10 EEG zu rechnen"

Qualitative und quantitative Schwellenwerte im Bereich "Stromversorgung" (Stand: 13. April 2016)

Anlagentyp	Kriterium	Im UP KRITIS erörterte Schwellenwerte			
Versorgungssicherheit	*Einwohneranzahl*	*250.000*	***500.000***	*1.000.000*	*2.000.000*
Erzeugungsanlagen	Leistung (MW)	210	**420**	850	1.700
Dezentrale Erzeuger	Leistung (MW)	210	**420**	850	1.700
Speicheranlagen	Leistung (MW)	210	**420**	850	1.700
Messstellen	Leistung (MW) +/-	210	**420**	850	1.700
Anlagen/Systeme zur Bündelung elektr. Leistung	Netto-Nennleistung (elektrisch) (MW)	210	**420**	850	1.700
Strombörse	n/a				
Übertragungsnetze	⌀ entnommene Leistung in MW/a	210	**420**	850	1.700
Verteilnetze	⌀ entnommene Leistung in MW/a	210	**420**	850	1.700

Schwachstellen des derzeitigen Entwurfs (1)

Betreiberbegriff nach § 1 Nr. 2 BSI-Kritisverordnung:

- "eine natürliche oder juristische Person, die unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände **bestimmenden Einfluss** auf die Beschaffenheit und den Betrieb einer Anlagen oder Teilen davon ausübt"
  - ➢ Betreiber einer Windenergieanlage (WEA) ./. IT-Dienstleister für WEA-Steuerung ./. White Labelling

Verordnungsbegründung:

- Betreiber ist nach immissionsschutzrechtlichem Verständnis regelmäßig der, der
  - …weisungsfrei und selbständig über Anlagen verfügt und…
  - …die tatsächliche Sachherrschaft über die Anlage besitzt, was meist mit der rechtlichen Verfügungsgewalt verknüpft ist, wer also…
  - …die Verfügungsgewalt in eigener Verantwortung ausübt

➢ Unbeachtlich, wenn sich Betreiber beim Betrieb der Anlage oder der erforderlichen IT-Systeme **IT-Dienstleister** bedient, sofern er bestimmenden Einfluss nicht aufgibt; Schwierigkeiten bereitet White Labelling

Schwachstellen des derzeitigen Entwurfs (2)

- Erfassung von Kritischer Dienstleistung **Bereitstellung von Regelleistung**
  - Systemdienstleistung dient als Marktmechanismus gerade zur Behebung netzrelevanter Störungen
  - Relevanz für Windenergie steigt seit Pilotverfahren zur Präqualifikation von Windenergieanlagen für negative MRL erheblich
  - Eingriffe insbesondere in Sekundär- oder Tertiärregelleistung kann bereits bei geringen MW-Mengen netzrelevante Störungen in deutschen Übertragungsnetzen begründen
  - Prüfung, ob IT-Anforderungen für Bereitstellung von Regelleistung bereits hinreichenden Sicherheitsmaßstab gewähren (dann jedoch ggf. von aus "Anlagen von Poolanbietern" auszuklammern)
- Erfassung weiterer **Systemdienstleistungen**
  - Anforderungen an Re-Dispatch Kraftwerke

Schwachstellen des derzeitigen Entwurfs (3)

- Überprüfung der **Schwellenwertbestimmung**
  - Abstellen auf **installierte Leistung** bei Erzeugungsanlagen an sich ungeeignet zur Bestimmung der Versorgungsgradrelevanz
    - Beinhaltet "tatsächlich möglicher Betriebsumfang" in Anhang 1 Teil 1 Nr. 4 auch wirtschaftlichen zumutbaren Anlageneinsatz bzw. tatsächliche Verfügbarkeit der Anlagen (soweit dargebotsabhängig)?
    - Windenergieanlagen und andere fluktuierende EEG-Anlagen werden nur mit geringen Volllaststunden eingesetzt, installierte Leistung hat wenig Aussagekraft für tatsächlichen/unmittelbaren Versorgungsgrad
  - Weitere Ausnahmen von Schwellenwertgrenzen (z. B. Speicher)

Schwachstellen des derzeitigen Entwurfs (4)

- Anwendungsbereich und -intensität hängt maßgeblich von **IT-Sicherheitskatalog** von BNetzA (im Benehmen mit BSI) ab
- IT-Sicherheitskatalog für Energieversorgungsnetze vom 12. August 2015 (Umsetzungsfrist 31. Januar 2018) als Blaupause für Energieanlagen?
  - Informationssicherheits-Managementsystem (ISMS)
  - Sicherheitskategorien/Maßnahmen nach DIN ISO/IEC 27002 u. TR 27019
  - Betrieb von IKT-Systemen und IKT-gestützten Verfahren und Prozessen
  - Netzstrukturplan (Leitsysteme/Systembetrieb, Übertragungs- und IKT-Technik, Sekundär-, Automatisierungs- und Fernwirktechnik)
  - Risikomanagement / Risikoeinschätzung / Risikobehandlung
  - Ansprechpartner IT-Sicherheit

Rechtsfolgen von Verstößen und Prävention

Rechtsfolgen bei Verstößen gegen IT-Sicherheitspflichten (1)

1. Rechtsfolgen für das Unternehmen

- Behördliche Aufsichtsmaßnahmen und Anordnungen (§ 65 Abs. 1, 2 EnWG); Vollstreckung in Form von Zwangsgeld möglich (§ 94 EnWG); aber **kein Bußgeld**
- Zivilrechtliche Haftung gegenüber Dritten aus Vertrag und ggf. Delikt
  - Schadensersatz wegen Verzug oder Nichterfüllung, Konventionalstrafen
  - Verletzung von Geheimhaltungsvereinbarungen: Schadensersatz wegen Vertragspflichtverletzung nach § 280 BGB
  - Falls Empfänger kein Vertragspartner: Schadensersatz nach § 823 BGB wegen Eigentumsverletzung
  - § 823 Abs. 2 BGB i.V.m. SchutzG (§§ 11 EnWG, 8a BSIG)?
  - ➢ Ausnutzung von Haftungsbegrenzungsmöglichkeiten und Sicherstellung IT-Compliance in Kunden- und Outsourcing-Verträgen

Rechtsfolgen bei Verstößen gegen IT-Sicherheitspflichten (2)

2. Haftung der Geschäftsleitung

- **Aktiengesellschaft:** "Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden." (§ 91 Abs. 2 AktG)
  - Bei Sorgfaltspflichtverletzung persönliche Haftung von Vorstandsmitgliedern
  - Beweislast für sorgfältiges Handeln bei Vorständen
  - ➢ Auch Haftung des **Aufsichtsrats** bei mangelnder Kontrolle (§§ 116, 111 AktG)
- **GmbH**: Anwendung der Sorgfalt eines ordentlichen Kaufmanns
  - § 43 Abs. 1 GmbHG: Sorgfalt eines ordentlichen Kaufmanns
  - § 43 Abs. 2 GmbHG: Schadensersatzpflicht gegenüber der Gesellschaft
- Bei Versicherungen und Banken weitere Organisations- und Überwachungspflichten aus § 64a VAG und § 25 a KWG

Rechtsfolgen bei Verstößen gegen IT-Sicherheitspflichten (3)

3. Maßnahmen zur Haftungsvermeidung und Sicherung von IT-Compliance:

- ✓ Einrichtung Risiko- und IT-Sicherheitsmanagement (ISMS)
- ✓ Einrichtung zentrale Kontakt-, Kommunikations- und **Meldestruktur**
- ✓ Erstellung IT-Sicherheitsleitlinien
- ✓ Umsetzung marktgerechter IT-Lösungen (u. a. technischer Datenschutz, Datenformate, Schnittstellen und Protokolle, Passwortschutz)
- ✓ Auswahl kompetenter Mitarbeiter; Schulung bestehender Mitarbeiter
- ✓ Bereitstellung angemessenes Sicherheits-Budget
- ✓ Regelmäßige Überprüfung der IT-Sicherheit (z. B. Penetrationstests)
- ✓ Umsetzung der Anforderungen auch durch IT-Dienstleister
  - ➢ Nachweis des Abschlusses marktgerechter IT-Outsourcingverträge

Outsourcing auf IT-Dienstleister

Outsourcing von Verantwortung auf einen IT-Dienstleister (1)

Grenzen bei der Einschaltung von Dienstleistern durch das IT-Sicherheits-gesetz?

- Keine Auslagerung von "Kernfunktionen" (vgl. § 25 b KWG)?
- (teilweise) Auslagerung der Verantwortung für einzelne Bereiche der Kritischen Infrastrukturen möglich!

Aber:

- Keine Exkulpationsmöglichkeit des Betreibers bei Verstoß – Verantwortung des Betreibers bleibt unberührt
  - Strenge Überwachungspflicht; ggf. Ausübung durch Dritte
  - Sicherstellung von Regressansprüchen
  - ➢ Vertragsgestaltung von zentraler Bedeutung!

Outsourcing von Verantwortung auf einen IT-Dienstleister (2)

1. Die **Auswahl** des Anbieters
   - Ausschreibung
   - IT-Sicherheitskonzept als maßgebliches Auswahlkriterium
2. Der **Outsourcing-Vertrag**
   - Weitergabe der Anforderungen aus IT-Sicherheitsgesetz bzw. branchenspezifischen Sonderregeln (z.B. technische und organisatorische Maßnahmen – toM, vgl. § 9 BDSG)
   - Unzureichender Vertrag als Verstoß gegen gesetzliche Anforderungen (z.B. Sorgfalt eines ordentlichen Kaufmanns)!
   - Pflicht zur Anpassung auch von Altverträgen

Outsourcing von Verantwortung auf einen IT-Dienstleister (3)

1. Leistungsbeschreibung
   - "Generalklausel" reicht nicht – Konkrete Vorgaben erforderlich, z.B. ISMS Umsetzung
   - Nutzung eigener Infrastruktur vs. Nutzung der Infrastruktur des Anbieters (SAAS)
   - Regelungen des Service Levels (SLA), insb. Verfügbarkeit und Integrität
   - Migrationsrechte auf redundante (Backup) Systeme des Anbieters / eigene Systeme
2. Change Management (regelmäßige Anpassung an regulatorisches Umfeld)
3. Informationspflichten, Audit und Zertifizierung
4. Haftung und Freistellung bei Verstößen gegen Sicherheitsanforderungen
   - Vereinbarung von Pönalen zur Durchsetzung der Pflichten
5. Kündigung und Exit Management
   - Zurückholen der Leistungen (z.B. Anlagenstammdaten und Erzeugungsdaten)
   - Sicherstellung effektive und vollständige Übertragung auf den Folgeanbieter

Vielen Dank für Ihre Aufmerksamkeit

Dr. Daniel Breuer
Rechtsanwalt

T +49 221 5108 4530
F +49 221 5108 4531

daniel.breuer@osborneclarke.com