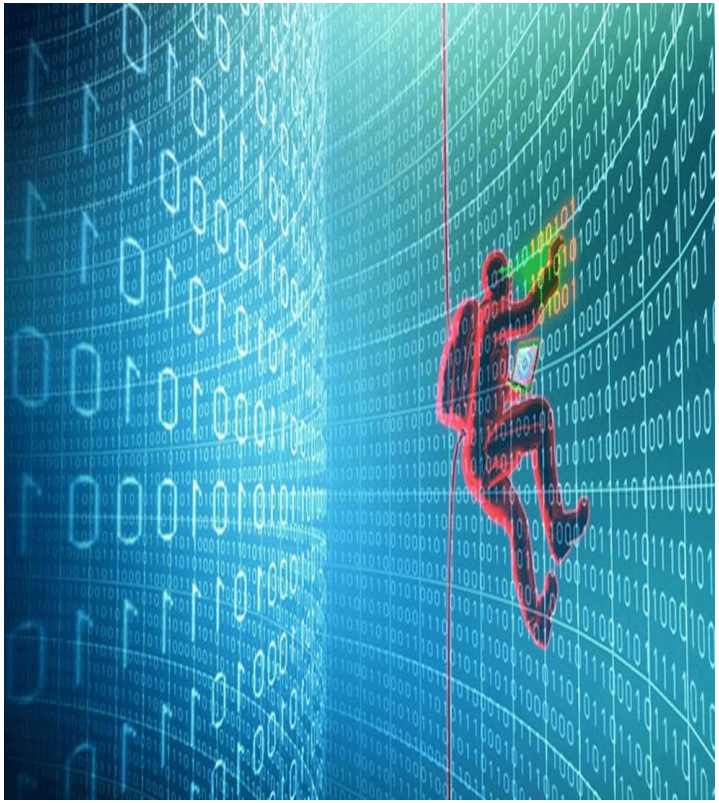
WOLTER HOPPENBERG Rechtsanwälte Partnerschaft mbB

IT-Sicherheitsgesetz – Chance oder Fluch?
Rechtlicher Rahmen, konkrete Anforderungen, praktische Umsetzung

- über 50 Rechtsanwälte, Steuerberater und Notare
- gegründet 1924
- Beratungsschwerpunkt öffentliche Hand, insb. Kommunen, Gebietskörperschaften und (kommunale) Unternehmen
- seit 20 Jahren Beratung der Energiewirtschaft
- bundesweit tätig

Ausgangslage für die neuen IT Sicherheitsanforderungen



Quelle:
http://images.computerwoche.de/images/computerwoche/bdb/1870275/986x555.png

- Die Nutzung von IT-Systemen und des Internets durchdringen Staat, Wirtschaft und Gesellschaft in immer größerem Maße. Neben den entstehenden Chancen wachsen jedoch auch Gefahren im Cyberraum. **Angriffe auf Staat, Verwaltung und Wirtschaft erfolgen zunehmend zielgerichtet** und sind technologisch immer ausgereifter und komplexer.

Ausgangslage für die neuen IT Sicherheitsanforderungen

- Der letzte medienwirksame Hacker-angriff galt im Frühsommer 2015 dem Deutschen Bundestag, der drei Monate lang nicht beendet werden konnte.
- Ergebnis:

  Die Systeme mussten komplett abgeschaltet und neu aufgesetzt werden.

- **Ziel des IT-Sicherheitsgesetzes** und des daraus resultierenden IT-Sicherheitskataloges der Bundesnetzagentur ist es, die informationstechnische Sicherheit deutlich zu verbessern und **kritische Infrastrukturen effektiver zu schützen**. Der Schutz von solchen kritischen Infrastrukturen ist von größter Wichtigkeit im Hinblick auf die Folgen eines Ausfalls oder der Beeinträchtigung ihrer Infrastruktur, die **dem Gemeinwohl verpflichtet** ist.

Kritische Infrastrukturen

Als kritische Infrastrukturen werden **alle Einrichtungen, Anlagen oder Teile** angesehen, die gem. § 1 Abs. 10 Nr. 1 **dem Sektor der Energie angehören** und nach Nr. 2 **von hoher Bedeutung für das Gemeinwesen sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden**.

- Diese kritischen Infrastrukturen werden durch die BSI-KritisV näher bestimmt.

Die BSI-KritisV sieht vor, dass Anlagen der Kategorien Energie, IT-Technik sowie für Wasser und Ernährung als kritische Infrastrukturen gelten. Dabei werden Schwellenwerte als Hilfsmittel eingesetzt, wie z.B.:

1. Wasserverteilungssystem ab 22 Mio. m³ pro Jahr
2. Wasserwerk ab 22 Mio. m³ Wasseraufkommen pro Jahr
3. Kläranlage ab 500.000 Einwohner, gemessen an der Ausbaugröße in Einwohnerwerten

Die Werte basieren auf einem Modell von 44 m³ Wasser pro Jahr und Bürger und einer Einwohneranzahl von 500.000.

Ausprägung der Schutzziele

Verfügbarkeit

Die Verfügbarkeit der zu schützenden Systeme und Daten muss sichergestellt sein, d.h. die Systeme und Daten dann **zugänglich und nutzbar** zu halten, wenn sie gefordert sind!

Integrität

Die Integrität der zu schützenden Systeme und Daten muss sichergestellt sein, d.h. **die Daten richtig und vollständig** zu halten und die **korrekte Funktionsweise der Systeme** zu verteidigen!

Vertraulichkeit

Die Vertraulichkeit der mit den betrachteten Systemen verarbeiteten Informationen muss gewährleistet sein, d.h. sie vor **unberechtigtem Zugriff durch Personen oder Prozesse** zu schützen.

Geltungsbereich des IT-Sicherheitskataloges

Der Geltungsbereich […] umfasst alle zentralen und dezentralen Anwendungen, Systeme und Komponenten, die für einen sicheren Netzbetrieb notwendig sind.

Enthalten sind demnach zumindest alle TK- und EDV-Systeme, die direkt Teil der Netzsteuerung sind […]. Auch betroffen sind solche Netzteile, die nicht direkt Teil der Netzsteuerung sind, deren Ausfall die Sicherheit des Netzbetriebs gefährden könnte.

Die Ermittlung der im Einzelfall betroffenen Systeme erfolgt durch den Netzbetreiber.

- Die betroffenen TK- und EDV-Systeme sind **vom Betreiber des Energieversorgungsnetzes** zu **identifizieren**.
- Nicht direkt an der Netzsteuerung beteiligte, dennoch **sicherheitsrelevante Anlagen** sind z.B. Messeinrichtungen an Trafo- oder Netzkoppel-stationen.
- Stets zu beachten sind **Messsysteme nach § 21d EnWG** zu **netzbetrieblichen Zwecken** wie der Ermittlung von Netzzustandsinformationen und der Ermöglichung von Last- und Erzeugungs-management.

Geltungsbereich des IT-Sicherheitskataloges

Der Geltungsbereich […] umfasst alle zentralen und dezentralen Anwendungen, Systeme und Komponenten, die für einen sicheren Netzbetrieb notwendig sind.

Enthalten sind demnach zumindest alle TK- und EDV-Systeme, die direkt Teil der Netzsteuerung sind […]. Auch betroffen sind solche Netzteile, die nicht direkt Teil der Netzsteuerung sind, deren Ausfall die Sicherheit des Netzbetriebs gefährden könnte.

Die Ermittlung der im Einzelfall betroffenen Systeme erfolgt durch den Netzbetreiber.

- Verantwortlich ist der Netzbetreiber. Werden Anwendungen, Systeme oder Komponenten **durch Dritte betrieben**, ist die Anwendung des IT-Sicherheitskataloges durch **vertragliche Vereinbarungen** sicherzustellen.

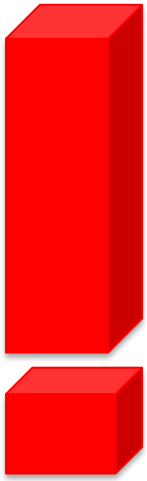
- **Die volle Verantwortung bleibt beim Betreiber des Energieversorgungsnetzes!**

Geltungsbereich des IT Sicherheitskataloges

- Da insbesondere **kleinere Netzbetreiber** selbst keine netzsteuernden oder sicherheitsrelevanten Systeme betreiben und diese an Dritte ausgegliedert haben, hat die BNetzA nun reagiert und die Pflicht zur Zertifizierung konkretisiert:

Werden sicherheitsrelevante Systeme vollständig oder teilweise durch den Netzbetreiber selbst betrieben, so ist die Zertifizierung notwendig.

Werden keine sicherheitsrelevanten Systeme betrieben oder sind diese vollständig an zertifizierte Dritte ausgelagert, ist eine Risikoanalyse als Nachweis zu erbringen, eine Zertifizierung jedoch entbehrlich.



1 Ausgangslage für die neuen IT-Sicherheitsanforderungen

2 Schutzziele

3 Geltungsbereich

4 Sicherheitsanforderungen

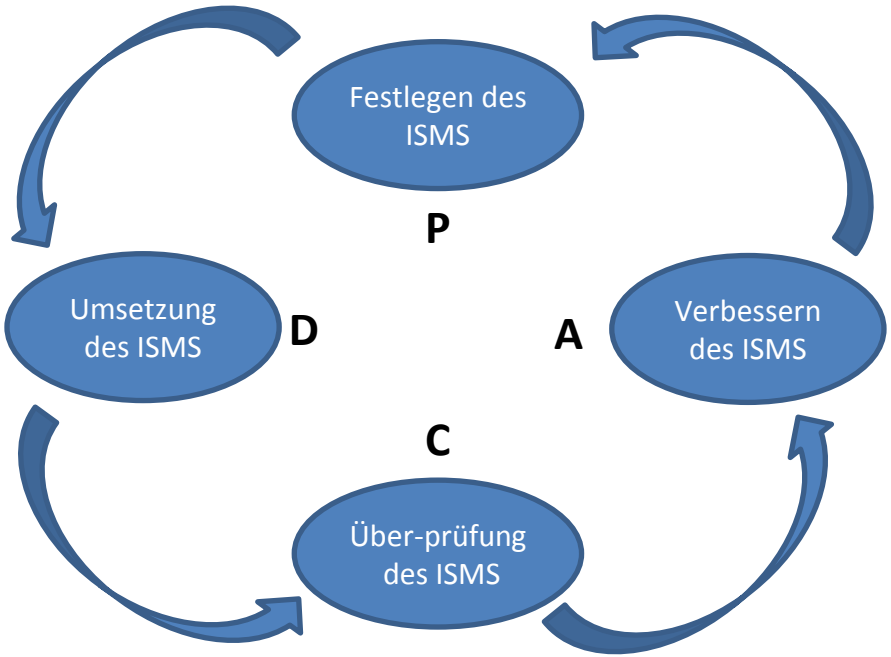
5 Fristen

6 Chancen und Herausforderungen ergreifen

Sicherheitsanforderungen

1. Informationssicherheits-Managementsystem (ISMS)

- Um Energieversorgungsunternehmen vor IT-Risiken effektiv zu schützen, sieht der Gesetzgeber einen **ganzheitlichen Ansatz** in der **Implementierung eines ISMS Systems** vor, welches mindestens den Anforderungen der **DIN ISO/IEC 27001** genügt.
- Die damit verbundenen Maßnahmen sind auf ihre Wirksamkeit hin in entsprechenden **Audits** zu überprüfen und ggf. anzupassen.
- Der Gesetzgeber empfiehlt einen regelmäßigen Prozess im **„Plan-Do-Check-Act-Modell“** (PDCA-Modell).
- Ziel ist die **Zertifizierung** nach der DIN ISO/IEC 27001.



Sicherheitsanforderungen

1. Informationssicherheits-Managementsystem (ISMS) – Beispielmaßnahmen

1. Operationalisieren!
Den Risikobehandlungsplan gilt es in technische Maßnahmen umzusetzen und darauf zu achten, dass die Langlebigkeit der Anlagen und damit verbundene vertragliche Konstellationen sowie relativ kurze Revisionszeiten abgebildet sind.

2. Zentrale Dienste etablieren!
Zentrale Dienste können z.B. Viren- und Patchmanagement-Lösungen beinhalten und technologieübergreifend über Security-Gateways bereitgestellt werden.

Besonders schutzbedürftige Anlagen sollten im Sinne einer **Defense-in-Depth-Strategie** isoliert werden.

3. Monitoring!
Neben einem unabdingbaren Security-Monitoring empfiehlt sich die Einrichtung eines Ereignisprotokolls, welches sicherheitsrelevante Informationen eigenständig erfasst und mit eigener Intelligenz bewertet, um Angriffe frühzeitig zu erkennen und abzuwehren.

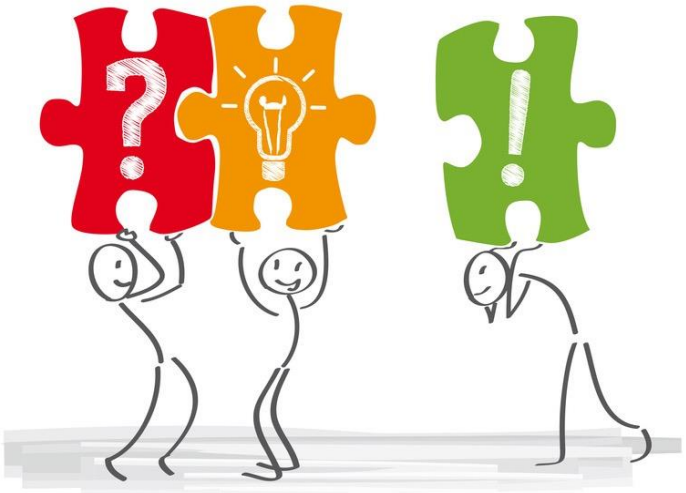
4. Weitere Maßnahmen:
- Mehrstufige Firewall
- Begrenzte Systemrechte
- Remote- und Fernzugriffe begrenzen
- Regelmäßige Back-Up‘s

Sicherheitsanforderungen

2. Sicherheitskategorien, Maßnahmen und ordnungsgemäßer Betrieb

- Bei der Implementierung des ISMS wird auf die Norm DIN ISO/IEC 27002 und DIN ISO/IEC TR 27019 verwiesen.
- Entscheidend für den Umgang mit den Verweisungen und der Umsetzung ist, diese **im Hinblick auf die Notwendigkeit für einen sicheren Netzbetrieb** anzuwenden.

- Die Vorgaben sind also **nicht ungeprüft umzusetzen**, sondern **im Sinne verantwortungsvoller Unternehmensführung** auf ihre **Bedeutung für die Sicherheit der Anlagen** hin zu etablieren.

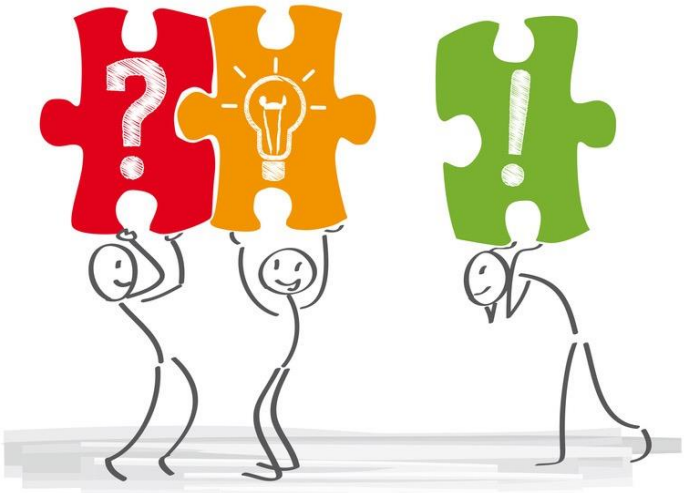


Quelle: http://www.sputnik-agentur.de/blog/was-ist-ein-kommunikationskonzept-und-brauche-ich-das/

Sicherheitsanforderungen

2. Sicherheitskategorien, Maßnahmen und ordnungsgemäßer Betrieb

- Entscheidend dafür ist **die Risikobewertung** der Anlagen
- Ziel ist es, dass die **eingesetzten Systeme und Anlagen** in ihren Verfahren und Prozessen **zu jedem Zeitpunkt beherrscht** werden **und Störungen als solche erkannt und behoben** werden können!



Quelle: http://www.sputnik-agentur.de/blog/was-ist-ein-kommunikationskonzept-und-brauche-ich-das/

Sicherheitsanforderungen

3. Der Netzstrukturplan

- **Der Netzbetreiber** hat eine **Übersicht über die** vom Geltungsbereich des IT-Sicherheitskatalogs betroffenen **Anlagen und Systeme mit den anzutreffenden Haupttechnologien** und deren Verbindungen zu erstellen. Dabei ist
  1. in Leitsysteme und Systembetrieb,
  2. Übertragungstechnik / Kommunikation sowie
  3. Sekundär- , Automatisierungs- und Fernwirktechnik

  zu gliedern.

- **Gruppenbildung** z.B. nach Typ, Konfiguration, Netz, Lokation, Anwendungen, Dienste etc. ist **zulässig und zur Vereinfachung sinnvoll.**

- Ebenso können **bei größeren Netzen getrennte Netzpläne** erstellt werden.

Tabelle 2: Technologiekategorien (Quelle: In Anlehnung an BDEW, S. 7 f.)

Technologie-kategorie	Beschreibung und Beispiele
Leitsysteme und Systembetrieb	Alle zentralisierten Systeme, die der Netzsteuerung und -überwachung dienen, sowie die hierzu notwendigen unterstützenden IT-Systeme, Anwendungen und zentralen Infrastrukturen zentrale Netzleit- und Netzführungssysteme zentrale Messwerterfassungssysteme Systeme zur Überwachung und Steuerung von Netzspeichern Datenarchivierungssysteme zentrale Parametrier-, Konfigurations- und Programmiersysteme die für den Betrieb der o. g. Systeme notwendigen , unterstützenden Systeme
Übertragungs-technik/ Kommunikation	Die in Netzsteuerung und Kommunikation eingesetzte Übertragungs-, Telekommunikations- und Netzwerktechnik. Beispiele: Router, Switches und Firewalls Übertragungstechnische Netzelemente Zentrale Management und Überwachungssysteme der Übertragungs-, Telekommunikations- und Netzwerktechnik Kommunikationsendgeräte Funksysteme
Sekundär-, Automatisier-ungs- und Fernwirktechnik	Die prozessnahe Steuerungs- und Automatisierungstechnik , die zugehörigen Schutz- und Sicherheitssysteme sowie fernwirktechnische Komponenten.

Sicherheitsanforderungen

4. Risikoeinschätzung und Risikobehandlung

Quelle: http://www.maniforex.de/wp-content/uploads/Risiko-und-Moneymanagement.jpg

- **Der Netzbetreiber hat einen Prozess zur Risikoeinschätzung festzulegen**, dem sich die Anlagen und Systeme im Hinblick auf die Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit ausgesetzt sehen.

- Dabei ist die Risikoeinschätzung in den bekannten Schadenskategorien zu bewerten:
  - „**Kritisch**“ (existentiell bedrohliches, katastrophales Risiko)
  - „**Hoch**“ (beträchtliche Schadensauswirkungen) und
  - „**Mäßig**“ (begrenzte, überschaubare Schadensauswirkung)

- Es gilt das sog. Ampelmodell

Sicherheitsanforderungen

4. Risikoeinschätzung und Risikobehandlung

- **Zu berücksichtigen** sind bei der Klassifizierung Kriterien wie die Beeinträchtigung der V**ersorgungssicherheit**, Einschränkungen des Energieflusses, **betroffener Bevölkerungsanteil**, **Gefährdung für Leib und Leben**, **Auswirkungen auf andere Infrastrukturen**, Gefährdung für D**atensicherheit und Datenschutz** und **finanzielle Auswirkung.**

Sicherheitsanforderungen

4. Risikoeinschätzung und Risikobehandlung

§ 11 Abs. 1 a EnWG:

Der Betrieb eines sicheren Energieversorgungsnetzes umfasst insbesondere auch einen **angemessenen Schutz gegen Bedrohungen** […], welcher für einen sicheren Netzbetrieb notwendig ist. […] **Ein angemessener Schutz** des Betriebs eines Energieversorgungsnetzes **liegt vor, wenn dieser Katalog der Sicherheitsanforderungen eingehalten und dies vom Betreiber dokumentiert worden ist.**

- Bei der Ermittlung der Risiken ist insbesondere auf folgende Ursachen zu achten:
  - Gezielte IT-Angriffe
  - Schadsoftware und Computerviren
  - Abhören von Kommunikation
  - Diebstahl von Rechnern usw.
- Auch gibt es Gefahren wie höhere Gewalt, menschliche Fehlhandlungen, technisches Versagen etc. die zu beachten sind.
- **Die herausgefilterten Risiken** müssen entsprechend behandelt werden. Darunter ist die Auswahl **geeigneter** und **angemessener Maßnahmen** zu verstehen.
- Hinsichtlich der Geeignetheit der Maßnahme ist auf den **„allgemein anerkannten Stand der Technik“** abzustellen.

Sicherheitsanforderungen

4. Risikoeinschätzung und Risikobehandlung

Stand der Technik

- Bei der Absicherung seiner Systeme hat der Netzbetreiber den **„allgemein anerkannten Stand der Technik“** zu berücksichtigen.
- Dieser unterliegt jedoch einer **hochdynamischen Entwicklung**.
- Auch sind nicht ungeprüft die neuesten Technologien zur Abwehr zu implementieren, sondern diese auf den Nutzen für die **individuelle Bedrohungslage** hin zu bewerten: Eine Frage der **Angemessenheit.**

§ 8a Abs. 1 BSIG:

Betreiber Kritischer Infrastrukturen sind verpflichtet, [...] **angemessene organisatorische und technische Vorkehrungen** zur Vermeidung von Störungen der IT-Systeme, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind zu treffen. **Dabei soll der Stand der Technik eingehalten werden.**

Sicherheitsanforderungen

4. Risikoeinschätzung und Risikobehandlung

Angemessenheit

- Ein **angemessener Schutz** liegt gemäß § 11 Absatz 1a S. 4 EnWG vor, **wenn der IT-Sicherheitskatalog eingehalten wird**.
- So gibt die BNetzA die Verantwortung ohne hilfreiche Hinweise zurück an die Betreiber.
- In die Ermittlung des individuellen Schutzbedarfes sind auch **Risiken der Sicherheit verbundener Netze einzubeziehen**.
- Zur Lösung ist ein insgesamt und ganzheitlich abgestimmtes **Vorgehen und Mitwirken der Branchenverbände in entscheidenden Gremien** gefragt.

§ 11 Abs. 1 a S. 4 EnWG:

Ein angemessener Schutz des Betriebs eines Energieversorgungsnetzes liegt vor, wenn dieser **Katalog der Sicherheitsanforderungen** eingehalten und dies vom Betreiber **dokumentiert** worden ist.

Sicherheitsanforderungen

5. Ansprechpartner

- Für die Koordination und Kommunikation der IT-Sicherheit **gegenüber der Bundesnetzagentur hat der Netzbetreiber einen Ansprechpartner zu benennen.**
- Dieser hat **auf Anfrage** unverzüglich darüber Auskunft zu erteilen, wie weit die **Vorgaben des IT-Sicherheitskataloges umgesetzt** sind, **welche Art und Umfang aufgetretene Sicherheitsvorfälle** hatten und wie diesen **begegnet** wurde.
- Zudem ist der Ansprechpartner **verantwortlich für die Anbindung an Kommunikationsinfrastrukturen** für Lageberichte und Warnmeldungen sowie großflächiger IKT-Krisen.
- Der Ansprechpartner ist nach den Kriterien des **Sicherheitsüberprüfungsgesetzes** und der Sicherheitsüberprüfungsfeststellungsverordnung auszuwählen bzw. hat diese Gesetze zu ertragen.

Sicherheitsanforderungen

5. Ansprechpartner

http://www.svgehrde.de/html/ansprechpartner.html

- Zudem ist der Ansprechpartner **verantwortlich für die Anbindung an Kommunikations-infrastrukturen** für Lageberichte und Warnmeldungen sowie großflächiger IKT-Krisen.
- Der Ansprechpartner ist nach den Kriterien des **Sicherheitsüberprüfungsgesetzes** und der Sicherheitsüberprüfungsfeststellungsverord-nung auszuwählen bzw. hat diese Gesetze zu ertragen.

1 Ausgangslage für die neuen IT-Sicherheitsanforderungen

2 Schutzziele

3 Geltungsbereich

4 Sicherheitsanforderungen

5 Fristen

6 Chancen und Herausforderungen ergreifen

Fristen

- Der Ansprechpartner für die IT-Sicherheit war der Bundesnetzagentur
  bis zum 30. November 2015
  zu nennen an die E-Mailadresse:

  IT-Sicherheitskatalog@bnetza.de

- Zum **Nachweis** darüber, dass die Anforderungen des IT-Sicherheitskatalogs umgesetzt werden, hat der Netzbetreiber der Bundesnetzagentur

  bis zum 31. Januar 2018

  den Abschluss des **Zertifizierungsverfahrens** durch Vorlage einer Kopie des Zertifikats mitzuteilen.

Quelle: http://www.bankenvergleich.de/wp-content/uploads/frist-320x145.gif

1 Ausgangslage für die neuen IT-Sicherheitsanforderungen

2 Schutzziele

3 Geltungsbereich

4 Sicherheitsanforderungen

5 Fristen

6 Chancen und Herausforderungen ergreifen

Chancen und Herausforderungen nutzen!

- **Ziel des IT-Sicherheitskataloges** ist nicht die Betreiber von kritischer Infrastruktur mit neuen Aufgaben zu beschäftigen, sondern dient der **Aufrechterhaltung der Versorgungssysteme in einer zunehmend digitalisierten** und damit auch angreifbaren **Infrastruktur**.

- Als Netzbetreiber gilt es jetzt die Chance zu nutzen und den Kunden zu zeigen, dass man sich **als verantwortungsvoller Netzbetreiber** um die Sicherheit der Systeme kümmert und damit Versorgungssicherheit gewährleistet.

http://www.springerprofessional.de/servlet/contentblob/3031682/articleImg/728924.jpg

Chancen und Herausforderungen nutzen!

- **Die Entwicklung entsprechender Maßnahmen**, die mit Kosten verbunden sind, sollten als unternehmerisch wünschenswerte **Investition in die Versorgungssicherheit** kommuniziert werden.
- Entscheidend für den Erfolg ist, dass die Branche dem Thema abgestimmt begegnet.

Chancen und Herausforderungen nutzen!

- **Wichtig** ist, dass man in diesem Fall nicht „das Kleid von der Stange kauft“, sondern eine **maßgeschneiderte Lösung** findet, welche die jeweils unternehmenseigenen Variablen entsprechend berücksichtigt und **sich optimal in das Zusammenspiel verschiedener Systeme und Anlagen einfügt**.
- Verfolgt wird vom IT-Sicherheitskatalog ein **ganzheitlicher Ansatz**, nicht der „Zusammenkauf“ verschiedener Einzelmaß-nahmen wie Anti-Viren-Software und Firewalls.

http://bilder.wanted.de/b/68/55/21/26/id_68552126/tid_da/ein-massschneider-liefert-ihnen-ein-unikat-.jpg

Chancen und Herausforderungen nutzen!

- **„Flickschusterei“** in diesem Zusammenhang führt **zur Inkaufnahme** etwaiger **Lücken im Sicherheitssystem oder inkompatible Systemnutzungen**, die nachher teurer werden können als eine verantwortungsvolle Lösung, die vorab die Probleme erkennt und ihnen ganzheitlich entgegentritt.

Haftungsrisiken beachten !

Aktuelle Entwicklungen

- Auf Initiative des Landes Hessen berät der Bundesrat derzeit über die Einführung des §202e StGB, den sog. „digitalen Hausfriedensbruch“.

- Das Strafrecht schützt derzeit nur die Unversehrtheit von Daten, nicht aber die Integrität informationstechnischer Systeme selbst. Dieser Schutz setzt auch nicht früh genug an.

- Schadprogramme werden z.B. unbekannt installiert und davon aus werden dann die Computer gesteuert. Das Sich-Verschaffen und Vermieten der sog. Bot-Netze ist derzeit nicht strafbar.

Aktuelle Entwicklungen

- Absatz 4 des § 202e-E sagt: „Handelt der Täter in der Absicht, einen Ausfall oder eine Beeinträchtigung der Funktionsfähigkeit kritischer Infrastrukturen zu bewirken, so ist die Strafe Freiheitsstrafe von einem Jahr bis zu zehn Jahren.“

- Damit handelt es sich um ein Verbrechen und die Formulierungen des ITSG/BSIG werden konkret aufgenommen.

- Der präventiven Wirkung des ITSG auf Seiten des Betreibers einer KI würde mit dem §202e StGB ein repressiver Ansatz für potenzielle Störer beigefügt.

Ihr Ansprechpartner

Wolter Hoppenberg
Rechtsanwälte Partnerschaft mbB

Münsterstraße 1-3, 59065 Hamm
Hafenweg 14, 48155 Münster

RA Martin Brück von Oertzen
Fachanwalt für Handels- und Gesellschaftsrecht
Wirtschaftsmediator

Tel.: 02381 92122-471
Fax: 02381 92122-7061
Email: bvo@wolter-hoppenberg.de

www.wolter-hoppenberg.de