Umsetzung IT-SiG in den Ländern

Erfahrungen aus dem Bereich AtG

Betroffenheit im Nds. Umweltministerium

KRITIS-Sektoren

Wasser (Trinkwasserversorgung, Abwasserbeseitigung)

Energie (Kerntechnische Anlagen, Verteilnetze, Konventionelle Anlagen etc.)

IT-Sicherheitsgesetz und Verordnung

Gesetzt zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz, IT-SiG) (24.7.2015)
Änderungen in BSIG, AtG, EnWG, TMG, TKG […]

1. Verordnung durch BMI (2. Mai 2016)

Definition der quantitativen Faktoren für die KRITIS-Sektoren Energie (Strom-, Gas-, Kraftstoff- und Fernwärmeversorung), Informationstechnik - Telekommunikation, Ernährung, Wasser

Ländersicht: Aufgaben der Aufsichtsbehörden

1. Herstellung des Benehmens mit den in den Ländern zuständigen Aufsichtsbehörden bei der Feststellung der Eignung von branchenspezifischen Sicherheitsstandards durch das BSI

   § 8a Absatz 2 Satz 3 Nummer 2 BSIG, ab 2016, gilt nicht im Geltungsbereich TKG, EnWG, AtG

Ländersicht: Aufgaben der Aufsichtsbehörden

2. Herstellung des Benehmens mit den Aufsichtsbehörden bei der Beseitigung von Sicherheitsmängeln

   §8a Absatz 3 Satz 3 Nummer 2 BSIG, voraussichtlich ab 2018,
   gilt nicht im Geltungsbereich TKG, EnWG, AtG

Ländersicht: Aufgaben der Aufsichtsbehörden

3. Analyse der potentiellen Auswirkungen von Sicherheitslücken, Schadprogrammen, zu erfolgten oder versuchten Angriffen auf die Verfügbarkeit Kritischer Infrastrukturen in der Zusammenarbeit mit den Aufsichtsbehörden

   § 8b Absatz 2 Satz 1 Nummer 2 BSIG

Ländersicht: Aufgaben der Aufsichtsbehörden

4. Entgegennahme von Unterrichtungen zu Gefahren, Auswirkungen und dem Lagebild von der zentralen Meldestelle im BSI durch die Aufsichtsbehörden oder die zu diesem Zweck von den Ländern als zentrale Kontaktstelle benannten Behörden

   § 8b Absatz 2 Satz 1 Ziffer 4 Buchstabe c BSIG

Atomg

IT-SiG nimmt Änderung im AtG vor und regelt

das Meldewesen gegenüber dem BSI

Artikel 2

Änderung des Atomgesetzes

Nach § 40 des Atomgesetzes in der Fassung der Bekanntmachung vom 15. Juli 1985 (BGBl. I S. 1565), das zuletzt durch Artikel 2 Absatz 14 des Gesetzes vom 1. April 2015 (BGBl. I S. 434) geändert worden ist, wird folgender § 44b eingefügt:

„§ 44b

Meldewesen für die Sicherheit in der Informationstechnik

Genehmigungsinhaber nach den §§ 6, 7 und 9 haben Beeinträchtigungen ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einer Gefährdung oder Störung der nuklearen Sicherheit der betroffenen kerntechnischen Anlage oder Tätigkeit führen können oder bereits geführt haben, unverzüglich an das Bundesamt für Sicherheit in der Informationstechnik als zentrale Meldestelle zu melden. § 8b Absatz 1, 2 und 7 des BSI-Gesetzes sind entsprechend anzuwenden. Die Meldung muss Angaben zu der Störung sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, und der betroffenen Informationstechnik enthalten. Das Bundesamt für Sicherheit in der Informationstechnik leitet diese Meldungen unverzüglich an die für die nukleare Sicherheit und Sicherung zuständigen Genehmigungs- und Aufsichtsbehörden des Bundes und der Länder weiter.“

Meldepflicht durch IT-SiG

Meldepflicht direkt mit Inkrafttreten des IT-SiG
Meldung (gegenüber BSI)

Meldeschwelle für Meldungen sehr hoch
(Gefährdung oder Störung der nuklearen Sicherheit)

Bisherige Meldungen seit Inkrafttreten IT-SiG:
Geringes Meldeaufkommen (0)

IT-SiG vs. AtG

Kerntechnische Anlagen werden grundsätzlich als Kritische Infrastrukturen betrachtet.

Für kerntechnische Anlagen existiert bereits ein umfangreiches Regelwerk. Auch für IT-Sicherheit.

SEWD-IT-Richtlinie = Branchenspezifischer Standard

- seit 2013
- In Zusammenarbeit mit BSI erarbeitet
- Sehr umfangreicher Betrachtungsgegenstand: betrifft sämtliche IT einer Anlage (auch Büro-IT, Webseite etc.) unabhängig von Vernetzungsgrad
- 3 Jahre Umsetzungsfrist
  Im August 2016 wurden die IT-Sicherheitskonzepte vorgelegt, diese werden derzeit geprüft

Beispiel Gundremmingen

Schadsoftwarefund auf Industrie-PC in der Anlage

Keine Gefährdung der nuklearen Sicherheit, aber Verletzung von Arbeitsvorschriften

Meldung an BSI freiwillig (weder nach §44b AtG (IT-SiG) noch nach AtSMV)

(Verordnung über den kerntechnischen Sicherheitsbeauftragten und über die Meldung von Störfällen und sonstigen Ereignissen (Atomrechtliche Sicherheitsbeauftragten- und Meldeverordnung - AtSMV)

Ecken und Kanten

- Meldung an BSI: Meldeformular auch nach mehr als einem Jahr noch nicht abgestimmt
- Betroffene Anlagen: sehr weit gefasst, auch im Rückbau befindliche Anlagen (ohne IT) betroffen

Zum Vergleich mit anderen KRITIS-Sektoren

- Klare Definition der Aufsichtsfunktion im Bereich AtG
  (in anderen KRITIS-Sektoren teilweise komplexer)
- Niedriger Vernetzungsgrad
- Sehr detailliertes Regelwerk vorhanden
- Technische Expertise in Aufsichtsbehörden hoch
- Ausgeprägte Sicherheitskultur vorhanden, ISMS kein Fremdwort

Im Vergleich

Beispiel KRITIS-Sektor Wasser:

- Verschiedene zuständige Aufsichtsbehörden (Gesundheitsämter, Untere Wasserbehörden, Gewerbeaufsichtsämter)
- Notwendige technische Expertise zur Bewertung von Sicherheitsvorfällen ist in Aufsichtsbehörden kaum vorhanden
- Branchenspezifische Sicherheitsstandards noch in Arbeit

Herausforderungen für Betreiber

- Betreiber bislang hinsichtlich IT-Sicherheit nicht immer optimal aufgestellt
- Kleine IT-Budgets, hohe Investitionsstaus, lange Abschreibungszeiträume
- Begrenzte Verfügbarkeit von Dienstleistungen im Bereich IT-Sicherheit?
- Nur 2 Jahre zur Entwicklung branchenspezifischer Standards, deren Umsetzung und Auditierung

Herausforderungen für Landesverwaltungen

Zusammenarbeit der Aufsichtsbehörden mit BSI auf freiwilliger Basis.

Unscharfe Definition „Aufsichtsbehörde“ verlangt Koordinierung innerhalb der Landesverwaltungen

Tatsächliche Aufgaben für Aufsichtsbehörden noch nicht klar

Meldeaufkommen nicht absehbar (Erfahrungen aus dem Bereich AtG nicht übertragbar)

Ausblick: Grenzen des IT-SiG

Bestimmte Anlagentypen werden per Definition nicht als Teil kritischer Infrastrukturen betrachtet