ENGEMANN | PARTNER

Rechtsanwälte und Notare

Angriffserkennung für kritische Infrastrukturen

WINDENERGIETAGE
www.spreewind.de

Spreewind Forum 3 – Auf einen Schnack mit ENERTRAG

ENGEMANN | PARTNER

Rechtsanwälte und Notare

Martina Beese

Rechtsanwältin

Kastanienweg 9
59555 Lippstadt
02941-970033
m.beese@engemann-und-partner.de

Sprecherin AK Weiterbetrieb und Anlagensicherheit im BWE e.V.
Stellv. Arbeitskreisleiterin DIN NABau 18088-6 AK (WKP)
Sprecherin AK Tragstruktur im BWE e.V.
Mitglied im juristischen Beirat im BWE e.V.
Mitglied im Sachverständigen Beirat im BWE e.V.
Gründungsmitglied Verein der Sachverständigen erneuerbare Energien e.V.

Neu und bedrohlich...?!

- Vermutlich Cyberangriff Ursache der Störung der Fernwartung tausender WEA Februar 2022
- April 2022 weiterer Angriff auf IT-Systeme eines Wartungsunternehmens.
- Gesetzgeber ist die Gefährdungslage bewusst. Seit 2015 kontinuierliche Schaffung und Erweiterung von Vorschriften.
- Festlegung kritischer Infrastrukturen: Erzeugungsanlagen, Anlagen oder Systeme zur Steuerung und Bündelung elektrischer Leistung.
- Ziel: Vermeidung flächendeckender Stromausfälle

EE-Anlagen als Kritische Infrastruktur und rechtliche Grundlagen

BSI-Gesetz
(IT-Sicherheitsgesetz)

BSI-KritisV

EnWG

IT-Sicherheitskatalog der BNetzA

- **Ab 1. Januar 2022:**
- **Erzeugungsanlagen mit einer Nennleistung von >104 MW gelten als Kritische Infrastruktur.**
- **Betreiber von Anlagen zur Steuerung/Bündelung (Aggregatoren) mit Schwellenwert 104 MW (deutlich herabgesetzt)**
- **Steuernder Fernzugriff (Leitwarte, Netzbetreiber, Direktvermarkter) auf gepoolte Erzeugungsanlagen.**

Entwicklung der Schwellenwerte BSI-KritisV

Tend

- **BSI-KritisV (bis 31.12.2021): > 420 MW**
- **Referentenentwurf (nicht umgesetzt!): > 36 MW bzw. > 50 MW diskutiert**

4 MW

- **Glück gehabt, Schwellenwert noch nicht erreicht!**
- **Geschäftsführung obliegt die Betriebsorganisation der IT-Sicherheit (GmbHG, AktG)**
- **Erfüllung des „üblichen" Sorgfaltsmaßstabes**
  - **Zuordnung von IT-Sicherheit**
  - **Risikomanagement und Reporting-System**
  - **Beachtung technischer Regelwerke wie IT-Grundschutz, Handlungsempfehlungen des BSI (Basis-Anforderungen)**
  - **Umsetzung von Basismaßnahmen**

Seit 1. Mai 2023 : Pflicht zum Einsatz von Systemen zur Angriffserkennung

§ 8a BSI-Gesetz (auszugsweise)

(1) Betreiber Kritischer Infrastruktur sind verpflichtet […] angemessene organisatorische und technische **Vorkehrungen zur Vermeidung von Störungen und 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. […]

(1a) Die Verpflichtung nach Absatz 1 Satz 1, angemessene organisatorische und technische Vorkehrungen zu treffen, umfasst ab 1. Mai 2023 auch den Einsatz von **Systemen zur Angriffserkennung**. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollen dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen. […]

(3) Betreiber Kritischer Infrastrukturen haben die Erfüllung der Anforderungen nach den Absätzen 1 und 1a […] dem Bundesamt **nachzuweisen**. […]“

Einsatz von Systemen zur Angriffserkennung (SzA)

E | P

„Systeme zur Angriffserkennung im Sinne dieses Gesetzes sind durch technische Werkzeuge und organisatorische Einbindung unterstützte Prozesse zur Erkennung von Angriffen auf informationstechnische Systeme. Die Angriffserkennung erfolgt dabei durch Abgleich der in einem informationstechnischen System verarbeiteten Daten mit Informationen und technischen Mustern, die auf Angriffe hindeuten“
(§ 2 Absatz 9b BSIG)

- **Derartige Systeme stellen eine effektive Maßnahme zur (frühzeitigen) Erkennung von Cyber-Angriffen dar und unterstützen insbesondere die Schadensreduktion und Schadensvermeidung.**

- **Große Bandbreite an technischen und organisatorischen Maßnahmen zur Angriffserkennung.**

- **Gewisse Umsetzungsfreiheit für die Betreiber. (Zielbetrachtung)**

Lesen: Orientierungshilfe zum Einsatz von Systemen der Angriffserkennung - ww.bsi.bund.de

3 Stufen der Angriffserkennung nach dem BSI

Die technische Funktionalität eines Systems zur Angriffserkennung basiert auf Abläufen im Bereich:

Protokollierung

Rechtfolgen sind unlustig mit Blick auf Bußgeldrahmen:

- **Nachweise nicht oder nicht rechtzeitig erbracht**
- **bis zu 10 Mio. €**

Detektion

- Kontinuier
- Einsatz Scl
- Auswertur
- Automatis

- **Festlegung Umsetzungsgrad und Begründung von Abweichungen**
- **Bestätigung**
- **Auflistung aufgedeckter Sicherheitsmängel**

Reaktion

- Automatische Reaktion auf sicherheitsrelevante Ereignisse
- Automatisch melden
- Eingriff in Datenstrom

ENGEMANN | PARTNER

Rechtsanwälte und Notare

Bleiben Sie gesund!

Wir wünschen viel Erfolg bei der Umsetzung.