



# Verpflichtende Nachweisprüfung von Angriffserkennungssystemen für Betreiber kritischer Infrastrukturen und Erzeugungsanlagen

Die weiter fortlaufende Vernetzung von Infrastrukturen untereinander und die damit immer komplexer werdene Systemlandschaft erhöhen auch die Menge an Einfallstoren für potenzielle Angreifer. Betreiber kritischer Infrastrukturen und Erzeugungsanlagen sind im Rahmen von Advanced Persistent Threats häufig das Ziel von Cyber-Attacken.

Angreifer bewegen sich vor Entdeckung meist lange unbemerkt im Netzwerk und haben dabei die Möglichkeit, Daten abzugreifen, Einfallstore zu schaffen oder sich lateral zu bewegen. Um Angriffe schnellstmöglich zu entdecken und Gegenmaßnahmen treffen zu können, ist der Einsatz von Angriffserkennungssystemen unabdingbar.

## Neue Anforderungen

Für Sie als Betreiber einer kritischen Infrastruktur, eines Energienetzes oder Erzeugungsanlagen ergibt sich auf Grundlage unterschiedlicher gesetzlicher Vorgaben eine verpflichtende Nachweisprüfung für den effektiven Einsatz eines Systems zur Angriffserkennung gegenüber dem BSI.

Das BSI hat nach Novellierungen im BSIG und dem EnWG am 26.09.2022 den Entwurf zur Orientierungshilfe für die Nachweisprüfung von Systemen zur Angriffserkennung veröffentlicht. In dieser Orientierungshilfe sind die Grundlagen beschrieben, die bei der Planung und Umsetzung solcher Systeme zu berücksichtigen sind und durch eine unabhängige Stelle geprüft werden müssen. Dabei werden die Bereiche Protokollierung, Detektion und Reaktion betrachtet.

## Unsere Leistung

Wir unterstützen Sie bei der Projektierung für die Einführung und den Betrieb eines Angriffserkennungssystems unter Berücksichtigung der energiewirtschaftlichen Herausforderungen und den Belangen Ihres Unternehmens. Hierbei beachten wir die spezifischen Anforderungen des BSI und unterstützen Sie bei der Nachweiserbringung nach § 8a (1a) BSIG und § 11 (1e) EnWG.



### Planung

Bereits bei der Planung des Angriffserkennungssystems sollten strategische Überlegungen angestellt werden. Dies betrifft die Kritikalität der zu schützenden Systeme, Einsatzbereiche und Verantwortlichkeiten.



### Umsetzung

Auf Basis der Erkenntnisse aus der Planung und Anforderungen des BSI begleiten wir Sie bei der Einführung des Systems.



### Prüfung

Betroffen von der Pflicht zur Einführung und dem Nachweis eines Angriffserkennungssystems sind:

- Betreiber kritischer Infrastrukturen nach § 8a (1a) BSIG (Nachweispflicht ab 01.05.2023)
- Betreiber von Energieversorgungsnetzen nach § 11 (1e) EnWG (Nachweispflicht zum 01.05.2023)
- Betreiber von bestimmten Energieanlagen nach § 11 (1e) EnWG, wenn die Schwellenwerte der BSI-KritisV erreicht werden (Nachweispflicht zum 01.05.2023)

Wir unterstützen Sie im Rahmen der Projektierung, Einführung und bei der Nachweiserbringung und führen die Nachweisprüfung bei Ihnen durch.

Als prüfende Stelle wird die Treuhand Weser-Ems GmbH Wirtschaftsprüfungsgesellschaft tätig.



## Kontakt

Jörg Jaenichen  
jaenichen@treuhand.de  
0441 9710-391

einfach.effizient. Treuhand  
Unternehmensberatung GmbH & Co. KG  
Langenweg 55 · 26125 Oldenburg