

Themensammlung für FAQs im Sinne des AT-3SV- Elektrizität im Zuge des AK IKT-Sicherheit

A. FAQs

A.1 **Hat der Sektor Energie sektorenspezifische Sicherheitsvorkehrungen (3SV) iSv § 17 Abs. 2 NISG erstellt?**

Der Sektor „Energie“ iSv § 2 Z 1 NISG im Teilsektor „Elektrizität“ iSv § 4 Abs. 1 Z 1 NISV hat mit seinem Sektorenverband (Oesterreichs Energie) sektorenspezifische Sicherheitsvorkehrungen erarbeitet. Diese wurden, nach Antrag beim und Freigabe durch den Bundesminister für Inneres gemäß § 17 Abs. 2 NISG, mit dem Titel *„Sektorenspezifische Sicherheitsvorkehrungen für den Sektor Energie (AT-3SV-Elektrizität) im Sinne des §17 Abs. 2 NISG mit Einschränkung auf den Teilsektor Elektrizität im Sinne des § 4 Abs. 1 Z 1 NISV“* auf der Webseite von Oesterreichs Energie veröffentlicht.

A.2 **Was ist der „Stand der Technik“ im Sektor Energie?**

Laut § 17 Abs. 1 NISG haben die Betreiber wesentlicher Dienste Sicherheitsvorkehrungen zu treffen, welche den Stand der Technik berücksichtigen. Daher hat Oesterreichs Energie im Sektor Energie für den Teilsektor Elektrizität den Anwendungsbereich definiert, dafür sektorenspezifische Sicherheitsvorkehrungen ausgearbeitet und diese im AT-3SV-Elektrizität festgehalten. Der Stand der Technik ist ein sich verändernder Stand an Sicherheitsvorkehrungen, der regelmäßig innerhalb der Branche abgestimmt und von den Betreibern wesentlicher Dienste entsprechend dem Risiko und wirtschaftlich angemessen umgesetzt wird.

A.3 **Wie ist der AT-3SV-Elektrizität anzuwenden?**

Zur Anwendung des AT-3SV-Elektrizität muss dieser in einem formellen Prozess beim Betreiber wesentlicher Dienste im Sinne seines Managementsystems als Teil der Compliance definiert werden. Dieser ist entsprechend dem Risiko und wirtschaftlich angemessen anzuwenden. Für die Prüfer von Qualifizierten Stellen ist dieser die Grundlage für eine klare und eindeutige Überprüfung.

A.4 **Müssen sich alle Betreiber einer Branche, die einen wesentlichen Dienst im Sinne des NISG betreiben, an den vorhandenen AT-3SV-Elektrizität halten?**

Nur jene Betreiber wesentlicher Dienste im Sektor Energie, Teilsektor Elektrizität und anderer Sektoren oder Teilsektoren, die sich in ihrer internen Compliance freiwillig selbst dazu verpflichtet haben, müssen sich an den AT-3SV-Elektrizität halten.

A.5 Welche Auswirkungen hat ein neuer oder angepasster AT-3SV-Elektrizität, wenn dieser als Prüfgrundlage zur Erbringung von Nachweisen nach § 17 Abs. 3 NISG verwendet werden soll?

Der 3SV definiert den Scope und damit den Anwendungsbereich der sektorspezifischen Sicherheitsvorkehrungen. Sobald ein neu angepasster AT-3SV-Elektrizität von der Behörde (BM.I) abermals freigegeben wurde, ist die neue bzw. angepasste Version für die Betreiber wesentlicher Dienste ein Umsetzungsleitfaden

A.6 Wie wird die Aktualität des AT-3SV-Elektrizität sichergestellt?

Der AT-3SV-Elektrizität wird alle drei Jahre aktualisiert und auf der Website von Oesterreichs Energie zur Verfügung gestellt.

A.7 Wie geht der AT-3SV-Elektrizität mit den unterschiedlichen Netz- und Informationssystemen bei den Betreibern wesentlicher Dienste um?

Der AT-3SV-Elektrizität ist als Rahmenvorgabe zu verstehen, der den Betreibern wesentlicher Dienste die gebotene Flexibilität bietet, sich bestmöglich an die Vorgaben des BM.I anzupassen. Das Ziel ist daher, dass Betreiber wesentlicher Dienste mittels risikobasiertem Ansatz individuell ihre Sicherheitsvorkehrungen und Netz- und Informationssysteme planen und wirtschaftlich angemessen umsetzen.

A.8 Wie ist mit Dienstleistungen zur Aufrechterhaltung des wesentlichen Dienstes umzugehen, die an Dritte ausgelagert wurden?

Der jeweilige Betreiber wesentlicher Dienste ist für die Aufrechterhaltung des wesentlichen Dienstes verantwortlich.

Wenn sich ein Betreiber im NIS-Scope Dienstleister bedient (z.B. zum Betrieb von Rechenzentren), dann sind die sich aus dem AT-3SV-Elektrizität ergebenden Verpflichtungen, ergänzend zu den Sicherheitsvorkehrungen der NISV, vertraglich mit dem Dienstleister festzulegen. Werden durch den Betreiber selbst keine NIS-Assets für die Bereitstellung des wesentlichen Dienstes eingesetzt, sind die vertraglich übertragbaren Aufgaben gemäß NISG an den Dienstleister formell festzulegen. Dessen ungeachtet verbleibt die Verantwortung beim Betreiber des wesentlichen Dienstes.

Die Umsetzung und Einhaltung der Vereinbarungen sind vom Betreiber eines wesentlichen Dienstes beim Dienstleister sicherzustellen.

A.9 Was ist bei Beschaffungen von Netz- und Informationssystemen für den Betrieb des wesentlichen Dienstes zu beachten?

Der AT-3SV-Elektrizität verweist diesbezüglich auf das BDEW-OE-Whitepaper „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme“.

A.10 Mir ist aufgefallen, dass es möglicherweise ein Risiko für einen Betreiber wesentlicher Dienste oder für die gesamte Branche geben könnte. Wohin kann ich Informationen senden?

Die Branche versucht die Risiken so gering wie möglich zu halten. Sollte Ihnen etwas aufgefallen sein, dann können Sie sich gerne an folgenden Kontakt beim Austrian Energy CERT wenden:

<https://www.energy-cert.at>

E-Mail Sicherheitsvorfall: reports(at)energy-cert.at

E-Mail allgemeine Anfragen: team(at)energy-cert.at

Das Austrian Energy CERT leitet die relevanten Informationen an die zuständigen Stakeholder weiter.

Glossar /Abkürzungen

Bezeichnung	Erläuterung
Abs.	Absatz
AK	Arbeitskreis
AT-3SV-Elektrizität	Sektorenspezifische Sicherheitsvorkehrungen im Sinne des §17 Abs. 2 NISG
3SV	sektorenspezifische Sicherheitsvorkehrungen
BDEW	Bundesverband der Energie- und Wasserwirtschaft e. V.
BM.I	Innenministerium
BwD	Betreiber wesentlicher Dienste
EU	Europäische Union
FAQ	Frequently Asked Questions
IEC	International Electrotechnical Commission
IKT	Information- und Kommunikationstechnologie
ISO	International Organization for Standardization
iSd	im Sinne der/des
iSv	im Sinne von/vom
iVm	in Verbindung mit
NISG	Netz- und Informationssystemsicherheitsgesetz
NISV	Netz- und Informationssystemsicherheitsverordnung
OE	Oesterreichs Energie, die Marke des Vereins Österreichs E-Wirtschaft
Z	Ziffer