AT-3SV-Elektrizität

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

Versionsnummer: 1.4

Ausstellungsdatum: 24. Juni 2021

Österreichs E-Wirtschaft

Über Oesterreichs Energie

Oesterreichs Energie vertritt seit 1953 die gemeinsam erarbeiteten Brancheninteressen der E-Wirtschaft gegenüber Politik, Verwaltung und Öffentlichkeit. Als erste Anlaufstelle in Energiefragen arbeiten wir eng mit politischen Institutionen, Behörden und Verbänden zusammen und informieren die Öffentlichkeit über Themen der Elektrizitätsbranche.

Die rund 140 Mitgliedsunternehmen erzeugen mit rund 20.000 Mitarbeiterinnen und Mitarbeitern mehr als 90 Prozent des österreichischen Stroms mit einer Engpassleistung von über 25.000 MW und einer Erzeugung von rund 68 TWh jährlich, davon 72 Prozent aus erneuerbaren Quellen.

Inhalt

A Änderungshistorie 3

B Projektteam 3

C Abkürzungsverzeichnis / Glossar 4

D Einleitung 5

D.1 Anwendungsbereich dieses Dokumentes 5

D.2 Verbesserungsprozess des Dokumentes 5

E Gesetzliches Umfeld und Mindestanforderungen 6

F Technologiekategorien 6

G Zonenkonzepte 7

G.1 Beschreibung der Zone 5 – „Internet“ 8

G.2 Beschreibung der Zone 4 – „Office Netzwerk“ 8

G.3 Beschreibung der Zone 3 – „Leitsysteme/Systembetrieb“ 8

G.4 Beschreibung der Zone 2 – „Sekundär-, Automatisierungs- und Fernwirktechnik“ ... 8

G.5 Beschreibung der Zone 1 – „Aktoren und Sensoren“ 9

G.6 Beschreibung der Zone 0 – „Physische Prozesse“ 9

G.7 Beschreibung des Zonenübergangs Zone 3 <-> Zone 4 – „Übergang zwischen OT-Umgebung und IT-Umgebung“ 9

H Schutzziele 9

I Geltungsbereich beim Betreiber (NIS-Scope und NIS-Assets) 10

J Out-of-NIS-Scope 12

K Übertragung an Hersteller und Integratoren 12

L Risikoeinschätzung und Risikobehandlung (Risikomanagement) 12

M Übertragung von Pflichten an Dienstleister 13

Anhang I. Übersichtstabelle Sicherheitsvorkehrungen in relevanten Dokumenten 14

Anhang II. Literaturverzeichnis 16

A Änderungshistorie

Version	Datum	Bearbeiter	Kommentar
V1.0	31.08.2020	AS & TP	Version für Einreichung beim BM.I
V1.0.5	07.04.2021	AS & TP	Einarbeitung und Überarbeitung basierend auf Zwischenbericht vom 11. Feb 2021 des BVT
V1.1	07.04.2021	AS & TP	Überarbeitete abgestimmte Fassung
V1.2	21.04.2021	TP	Überarbeitung Tabelle ANHANG I
V1.3	22.04.2021	AS	Finale Version zur Rückmeldung an BVT
V1.4	24.06.2021	AS & TP	Finalisierte Version zur Übermittlung an BVT

B Projektteam

Ansprechpartner

Dipl.-Ing. Armin Selhofer, MSc (Österreichs E-Wirtschaft)

Projektleitung

Thomas Pfeiffer, BSc MSc (LINZ NETZ GmbH, Linz)

Mitwirkende

Mitarbeiter Oesterreichs Energie, Projektmitglieder Oesterreichs Energie und Ansprechpartner in den Unternehmen des Sektors Energie.

Trotz sorgfältiger Prüfung wird keine Gewähr für die inhaltliche Richtigkeit übernommen. Außer für Vorsatz und grobe Fahrlässigkeit ist jegliche Haftung aus dem Inhalt dieses Werks ausgeschlossen.

Diese Publikation ist urheberrechtlich geschützt.

Alle Rechte vorbehalten. © Wien 2021

C Abkürzungsverzeichnis / Glossar

Abkürzung	Beschreibung
3SV	Sektorenspezifische Sicherheitsvorkehrungen
Abs.	Absatz
AT	Austria
Bereiche	Die Bereiche beziehen sich auf den Teilsektor Elektrizität im Sektor Energie. Folgende Bereiche sind definiert: Stromerzeugung, Stromverteilung und Stromübertragung
BDEW	Bundesverband der Energie- und Wasserwirtschaft
E-Wirtschaft	Elektrizitätswirtschaft
IEC	International Electrotechnical Commission
IKT	Informations- und Kommunikationstechnologie
ISMS	Informationssicherheitsmanagementsystem
ISO	International Organization for Standardization
IT	Information Technology (Enterprise Network, Office Network, Büro-Netzwerk odgl.)
NIS	Netz- und Informationssystemsicherheit
NIS–Assets	Systeme, Objekte und Personen im definierten NIS-Scope des Betreibers von wesentlichen Diensten
NISG	Netz- und Informationssystemsicherheitsgesetz
NISV	Netz- und Informationssystemsicherheitsverordnung
NIS-Scope	Dem Risiko angemessener erhobener Geltungsbereich im Umfeld des Betreibers wesentlicher Dienste unter Einhaltung der in diesem Dokument definierten Bereiche.
OE	Oesterreichs Energie, Marke von Österreichs E-Wirtschaft
OT	Operational Technology (Industrial Control Systems, Prozessnetzwerk, Steuernetzwerk odgl.)
PPD	Public-Private-Dialog
SCADA	Supervisory Control And Data Acquisition
SPoC	Single Point of Contact / Kontakt- bzw. Meldestelle
SPS	Speicherprogrammierbare Steuerung
TLP	Traffic Light Protocol
Z	Ziffer

D Einleitung

Dieses Dokument ist im Auftrag von Oesterreichs Energie erstellt worden und soll die sektorenspezifischen Sicherheitsvorkehrungen für den Teilsektor Elektrizität (AT-3SV-Elektrizität) im Sinne des Netz- und Informationssystemsicherheitsgesetzes (NISG) [1] und der Netz- und Informationssystemsicherheitsverordnung (NISV) [2] definieren sowie eine vergleichbare Grundlage für die Definition des Geltungsbereichs (NIS-Scope) dieser Vorkehrungen durch die Betreiber wesentlicher Dienste festlegen.

Ebenfalls dient es als Grundlage für Prüfer oder qualifizierte Stellen, um die getroffenen Sicherheitsvorkehrungen klar und eindeutig überprüfen zu können.

Sämtliche Bezeichnungen sollen geschlechtsneutral verstanden werden. Wurde nur auf ein Geschlecht verwiesen, so gilt die Formulierung auch für alle anderen Geschlechter.

D.1 *Anwendungsbereich dieses Dokumentes*

Gemäß § 17 Abs. 2 erster Satz NISG können Betreiber wesentlicher Dienste und ihre Sektorenverbände sektorenspezifische Sicherheitsvorkehrungen zur Gewährleistung der Anforderungen nach § 17 Abs. 1 NISG vorschlagen.

Dieser vorliegende AT-3SV-Elektrizität kann für Betreiber wesentlicher Dienste im Teilsektor Elektrizität nach § 2 Z 1 NISG in Verbindung mit § 4 Abs. 1 Z 1 NISV spezifischer dem Teilsektor Elektrizität und innerhalb dessen Bereichen

- Stromerzeugung
  - Betrieb einer Erzeugungsanlage
  - Betrieb von Systemen zur Steuerung von Erzeugungsanlagen
- Stromverteilung
  - Betrieb eines Verteilnetzes
- Stromübertragung
  - Betrieb eines Übertragungsnetzes

Anwendung finden, welche mittels rechtsgültigem Bescheid im Sinne von § 16 Abs. 4 Z 1 NISG identifiziert wurden. 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.

D.2 *Verbesserungsprozess des Dokumentes*

Dieses Dokument soll ein Jahr nach der erstmaligen Veröffentlichung einer Überprüfung durch den Auftraggeber unterzogen werden und folglich in einem Zyklus von drei Jahren. Der Zyklus von drei Jahren kann sich verkürzen, wenn Sicherheitsvorfälle oder neue Erkenntnisse des Sektors dies erforderlich machen; sich insbesondere die Sicherheitsvorkehrungen in Verbindung mit NISV ändern; bei Änderungen von relevanten Standards oder falls bei Überprüfungen durch qualifizierte Stellen Unklarheiten entstehen. Eine aktualisierte Version aus diesem Verbesserungsprozess zieht einen erneuten Eignungsfeststellungsprozess durch den Bundesminister für Inneres mit sich.

E Gesetzliches Umfeld und Mindestanforderungen

Um die Bereitstellung des wesentlichen Dienstes sicherzustellen, hat dessen Betreiber in Hinblick auf die Netz- und Informationssysteme geeignete und verhältnismäßige technische und organisatorische Sicherheitsvorkehrungen zu treffen. Diese haben den Stand der Technik zu berücksichtigen und dem Risiko, das mit vernünftigem Aufwand feststellbar ist, angemessen zu sein. Bei der Anwendung der Sicherheitsvorkehrungen sind die in diesem Dokument angeführten Technologiekategorien zu berücksichtigen und haben ebenfalls dem Risiko, das mit vernünftigem Aufwand feststellbar ist, angemessen zu sein. Diese vorliegenden sektorenspezifischen Sicherheitsvorkehrungen bilden eine Erweiterung zu den Mindestanforderungen der NISV an Betreiber wesentlicher Dienste in prüfbare Anforderungen ab.

Um ein angemessenes Sicherheitsniveau für die Bereitstellung des wesentlichen Dienstes zu gewährleisten, ist die bloße Umsetzung von Einzelmaßnahmen nicht ausreichend. Zur Erreichung der Schutzziele ist ein ganzheitlicher Ansatz nötig, der kontinuierlich auf Leistungsfähigkeit und Wirksamkeit zu überprüfen und bei Bedarf anzupassen ist.

Um den Anforderungen für einen ganzheitlichen Ansatz und den Anforderungen laut § 11 NISV zu entsprechen, ist durch den Betreiber des wesentlichen Dienstes ein Informationssicherheitsmanagementsystem (ISMS) nach ISO/IEC 27001 in Verbindung mit der ISO/IEC 27002 unter Berücksichtigung der ISO/IEC 27019 sowie insbesondere für Beschaffungen das OE-BDEW-Whitepaper „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme“ mindestens im definierten Geltungsbereich (NIS-Scope) als organisatorische Maßnahme umzusetzen.

Im Kern bilden die Anforderungen der ISO/IEC 27001 in Verbindung mit der ISO/IEC 27002 unter Berücksichtigung der ISO/IEC 27019 und dem OE-BDEW-Whitepaper in der aktuell anwendbaren Fassung eine umfassende Grundlage zur Anwendung und werden zur Umsetzung des AT-3SV-Elektrizität vorgegeben. Der AT-3SV-Elektrizität erläutert die für den Teilsektor Elektrizität geeigneten Ergänzungen und Regelungen für technische und organisatorische Maßnahmen.

Der AT-3SV-Elektrizität regelt, dass die nachhaltige und angemessene Behandlung aller relevanten Themenfelder zur Umsetzung der rechtlichen Anforderungen sichergestellt ist, insb. nach § 17 Abs. 1 NISG in Verbindung mit NISV durch den Betrieb eines Informationssicherheitsmanagementsystems (ISMS), wie im vorliegenden Dokument beschrieben.

F Technologiekategorien

Der Teilsektor Elektrizität umfasst unterschiedliche Systeme. Um den relevanten spezifischen Geltungsbereich (NIS-Scope) zu formulieren, werden Kategorien von Technologien eingeführt.

Die folgenden Technologiekategorien decken die eingesetzten IKT- und OT-Systeme im Teilsektor Elektrizität ab. Die Technologien werden in Folge in die Kategorien „Leitsysteme/Systembetrieb“, „Übertragungstechnik/Kommunikation“ und „Sekundär-, Automatisierungs- und Fernwirktechnik“ eingeteilt. Tabelle 1 enthält eine kurze Beschreibung sowie einige Beispiele für Technologien.

Tabelle 1: Technologiekategorien in Anlehnung an BDEW/OE – Whitepaper [3]

Technologiekategorie	Beschreibung und Beispiele
Leitsysteme/ Systembetrieb	Systeme, die der Netzsteuerung und -überwachung oder der Steuerung von Erzeugungsanlagen dienen, sowie die hierzu notwendigen unterstützenden Systeme, Anwendungen und zentralen Infrastrukturen. Beispiele: - Netzleit- und Netzführungssysteme für Energieübertragung und -verteilung, - Warten zur Steuerung von Erzeugungsanlagen, - Zentrale Messwerterfassungssysteme, - Zentrale Parametrier-, Konfigurations- und Programmiersysteme.
Übertragungstechnik/ Kommunikation	Die in der Steuerung von Netzen oder Erzeugungsanlagen zur Kommunikation eingesetzte Übertragungs-, Telekommunikations- und Netzwerktechnik. Beispiele: - Router, Switches und Firewalls, - Fernwartungssysteme, - Übertragungstechnische Netzelemente, - Management-, Konfigurations- und Überwachungssysteme der Übertragungs-, Telekommunikations- und Netzwerktechnik.
Sekundär-, Automatisierungs- und Fernwirktechnik	Die prozessnahe Steuerungs- und Automatisierungstechnik, die zugehörigen Schutz- und Sicherheitssysteme, fernwirktechnische Komponenten sowie die Automatisierungstechnik Beispiele: - Örtliche Stations- oder Wartenleittechnik, - Steuerungs- und Automatisierungskomponenten, - Leit- und Feldgeräte, - Controller und SPSen inklusive digitaler Sensor- und Aktorelemente, - Schutzgeräte und Sicherheitskomponenten, - Fernwirkgeräte, - Mess- und Zählvorrichtungen, mit Ausnahme jener, welche für Verrechnungen des Energieverbrauches dezentral bei juristischen oder natürlichen Personen installiert sind, - Parametrierungs- und Programmierwerkzeuge.

G Zonenkonzepte

Die Technologiekategorien sind den nachfolgend abgebildeten Zonen zugeordnet oder dienen als Kommunikationskanäle an den Übergängen von einer Zone in eine andere. Eine Zone ist eine Gruppierung von Systemen. Ein Überblick über die Zonen und den relevanten Übergang von der IT- in die OT-Umgebung sowie die zugeordneten Technologiekategorien werden in Abbildung 1 dargestellt.

Abbildung 1: Zonendarstellung mit Technologiekategorien

Die Systeme der Zonen 5 und 4 werden als „Informationstechnik“ (IT) bezeichnet. Die Systeme der Zonen 3 bis 0 werden als „Operational Technology“ (OT) bezeichnet.

G.1 *Beschreibung der Zone 5 – „Internet“*

Zone 5 wird als allgemeine, unsichere Zone bezeichnet. Hier sind z.B. das öffentliche „Internet“ oder andere öffentliche Kommunikationsnetze im Sinne § 3 Z 1 lit. a NISG angesiedelt.

G.2 *Beschreibung der Zone 4 – „Office Netzwerk“*

In der Zone 4 befinden sich Systeme und Prozesse, die für den kaufmännischen Geschäftsbetrieb notwendig sind.

G.3 *Beschreibung der Zone 3 – „Leitsysteme/Systembetrieb“*

In der Zone 3 befinden sich Systeme der Technologiekategorien „Leitsysteme/Systembetrieb“ bzw. „Übertragungstechnik/Kommunikation“.

G.4 *Beschreibung der Zone 2 – „Sekundär-, Automatisierungs- und Fernwirktechnik“*

In der Zone 2 befinden sich die Systeme der Technologienkategorien „Sekundär-, Automatisierungs- und Fernwirktechnik“ bzw. „Übertragungstechnik/Kommunikation“.

G.5 *Beschreibung der Zone 1 – „Aktoren und Sensoren“*

In der Zone 1 befinden sich Sensoren und Aktoren, welche zur Gewinnung von Informationen aus dem Bereich der materiellen Produktion dienen bzw. Einfluss auf die physischen Prozesse nehmen.

G.6 *Beschreibung der Zone 0 – „Physische Prozesse“*

In der Zone 0 befinden sich die physischen Prozesse wie z.B. elektrische Energietechnik.

G.7 *Beschreibung des Zonenübergangs Zone 3 <-> Zone 4 – „Übergang zwischen OT-Umgebung und IT-Umgebung“*

Alle Schnittstellen zwischen den Zonen 3 und 4 müssen miteinbezogen werden. Dazu zählen die Fernwartungszugänge zu den OT-Umgebungen, die Sicherheitsvorkehrungen an dem Zonenübergang (z.B. Firewall, Protokollfilter) und der Einsatz von mobilen Geräten (z.B. Engineering-Laptop eines Systemtechnikers).

In Abbildung 2 sind Systeme, Technologiekategorien, Beispiele von Systemen und relevanten Schnittstellen in IT- und OT-Umgebungen generisch dargestellt.

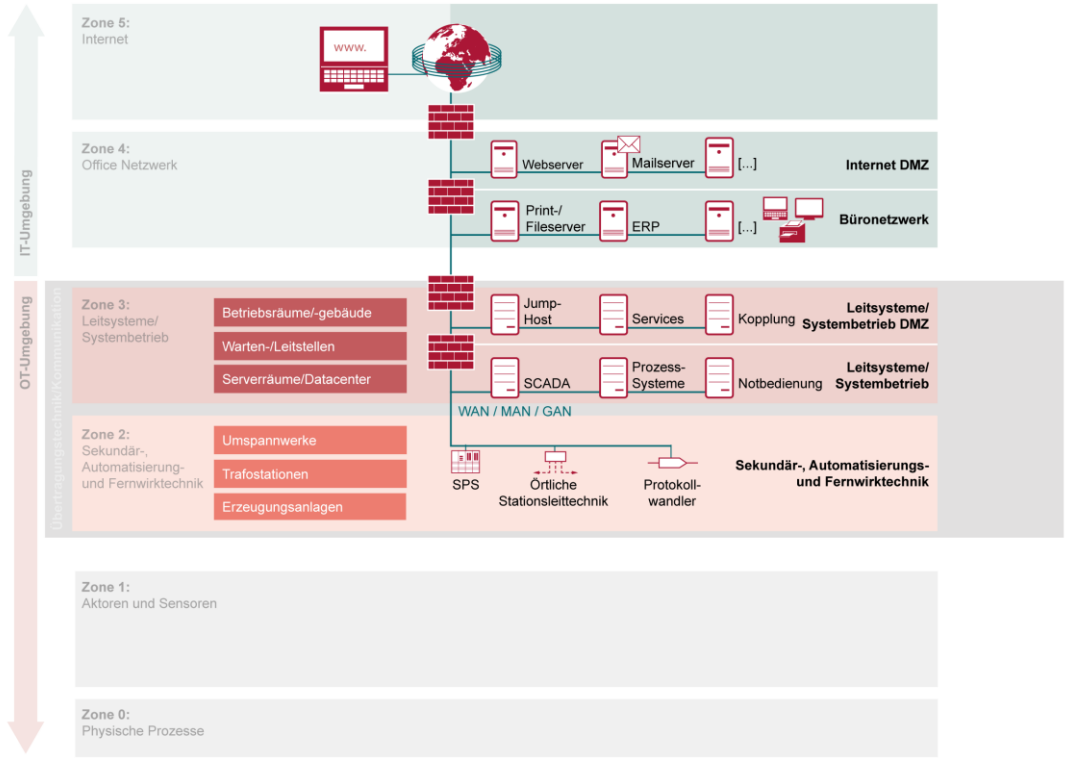

Abbildung 2: Generischer Strukturplan mit Zonen und Technologiekategorien

H Schutzziele

Für Betreiber wesentlicher Dienste im Sinne des AT-3SV-Elektrizität werden Schutzziele für die Bereitstellung des wesentlichen Dienstes definiert.

Die Schutzziele umfassen ganzheitlich alle geeigneten und verhältnismäßigen, technischen und organisatorischen Sicherheitsvorkehrungen gegen Gefährdungen der jeweiligen Technologiekategorien, die für die Bereitstellung des wesentlichen Dienstes notwendig sind.

Diese haben den Stand der Technik zu berücksichtigen und dem Risiko, das mit vernünftigem Aufwand feststellbar ist, angemessen zu sein.

Aufbauend auf diesen Schutzzielen sind im Rahmen des ISMS nach ISO/IEC 27001 in Verbindung mit der ISO/IEC 27002 unter Berücksichtigung der ISO/IEC 27019 anlagenspezifische Informationssicherheits-Anforderungen abzuleiten und ebenfalls dem Risiko angemessen zu berücksichtigen.

I Geltungsbereich beim Betreiber (NIS-Scope und NIS-Assets)

Der Geltungsbereich (**NIS-Scope**) des vorliegenden AT-3SV-Elektrizität umfasst zumindest jene zentralen und dezentralen Assets, die für die Bereitstellung des wesentlichen Dienstes im Teilsektor Elektrizität erforderlich sind. Eine schematische Darstellung des harmonisierten NIS-Scopes für die Betreiber wesentlicher Dienste ist Abbildung 3 zu entnehmen.

Assets, welche sich im NIS-Scope befinden oder als Schnittstellen dazu definiert sind und für die Bereitstellung des wesentlichen Dienstes notwendig sind, werden als **NIS-Assets** bezeichnet und können in mindestens eine der drei in Tabelle 2 beschriebenen Kategorien eingeordnet werden.

Tabelle 2: Beschreibung der Kategorien für NIS-Assets in Anlehnung an das Österreichische Informationssicherheitshandbuch [4]

NIS-Asset	Beschreibung
Systeme	Diese Assets werden in den Technologiekategorien (Siehe Tabelle 1 auf Seite 7) mit Beispielen angeführt.
Objekte	Zu diesen Assets zählen Gebäude, Räume oder auch Schaltschränke in welchen sich Systeme befinden.
Personen	Zu diesen Assets zählen Personen welche sich in Objekten aufhalten oder auf Systeme vor Ort bzw. aus der Ferne zugreifen können und für die Bereitstellung des wesentlichen Dienstes entscheidend sind.

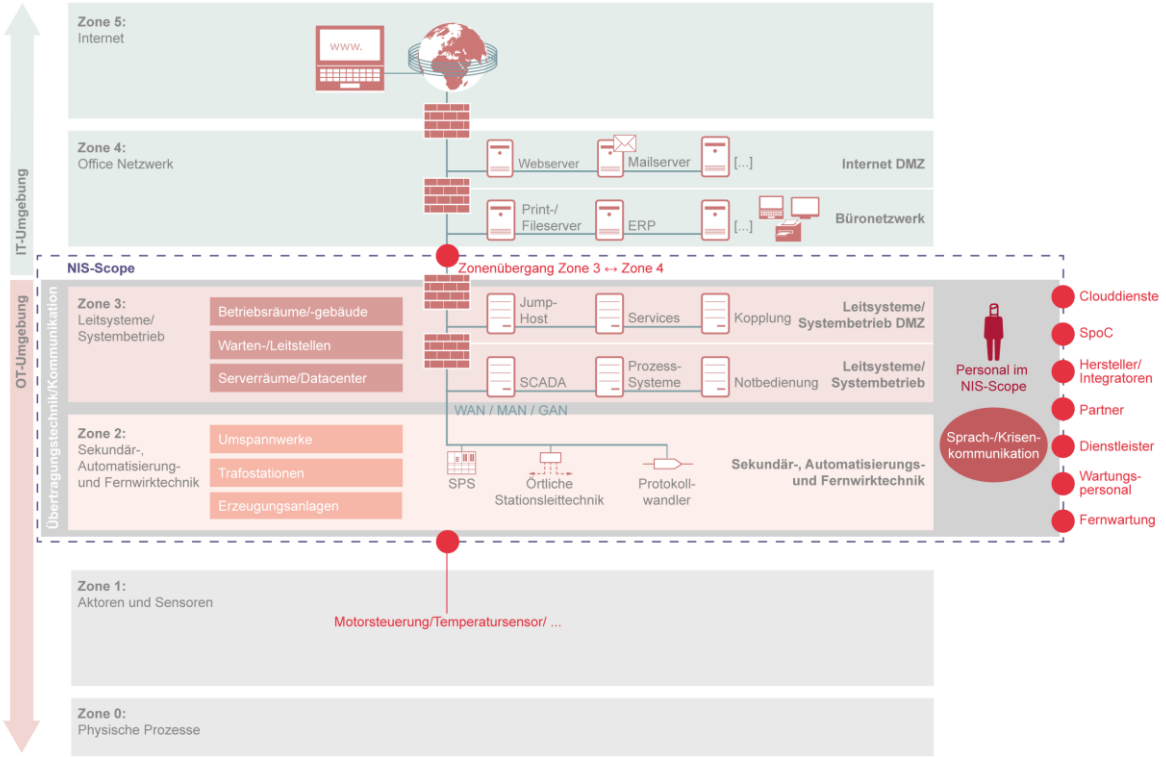

Abbildung 3: NIS-Scope inklusive Assets und Schnittstellen

Die Ermittlung der betroffenen NIS-Assets in den Zonen 2 und 3 erfolgt in einem risikobasierten Ansatz durch den jeweiligen Betreiber selbst und kann unternehmensabhängig divergieren.

Dazu kann, abhängig von den jeweiligen Unternehmensaufgaben und -zielen, eine Unterteilung in zentrale und dezentrale Anlagen erfolgen. Ebenfalls sind Gruppierungen von NIS-Assets erlaubt.

Es sollen in der Folge auch zumindest jene einzelnen Anlagen bzw. Betriebsstandorte abhängig von den Kriterien entsprechend des gültigen Ermittlungsbescheides in den Geltungsbereich (NIS-Scope) aufgenommen werden.

Für alle Betreiber wesentlicher Dienste der definierten Bereiche im Teilsektor Elektrizität gilt, dass zumindest jene Technologiekategorien betroffen sind, welche für die Bereitstellung des wesentlichen Dienstes erforderlich sind.

Damit ergibt sich, dass zumindest diejenigen Assets des Betreibers, welche für die Messung- und Überwachung von Erzeugungs- und Netzanlagen bzw. die Steuerung und Regelung der elektrischen Leistung, des Einspeiseverhaltens und/oder der verteilten bzw. übertragenen Energiemenge essentiell sind, als NIS-Assets im Sinne der vorliegenden Sicherheitsvorkehrungen gelten.

Insbesondere umfasst dies Bestandteile wie zum Beispiel SCADA-Applikationen, Regelungs- und Steuerungskomponenten, Schutzsysteme, Fernwirkgeräte, Energiemanagement- und Überwachungssysteme oder zentrale Datenbanken mit betrieblich notwendiger, direkter Anbindung an das Steuer- / Leitsystem.

Zusätzlich sind die zum Betrieb der oben genannten Technologiekategorien und zur Kommunikation mit den Erzeugungs- oder Netzanlagen und angeschlossenen Netzbetreibern notwendigen zentralen Netzwerke, Firewalls, Gateways, Router etc. als NIS-Assets zu betrachten.

J Out-of-NIS-Scope

Nicht in den Geltungsbereich (NIS-Scope) gehören vorgelagerte zentrale oder dezentrale Systeme des Energiehandels oder der klassischen Marktkommunikation und Assets bzw. Gruppen von Assets, welche nach dem risikobasierten Ansatz nicht für die Bereitstellung des wesentlichen Dienstes notwendig sind, obwohl diese den Zonen 3 oder 2 zugeordnet sind. Dies ist nachvollziehbar zu begründen.

K Übertragung an Hersteller und Integratoren

Im Zuge einer Neubeschaffung von NIS-Assets müssen die in diesem Dokument definierten Vorgaben berücksichtigt werden. Bei zukünftigen Ausschreibungen von Systemen für den Einsatz im NIS-Scope ist das von OE/BDEW publizierte „Whitepaper Anforderungen an sichere Steuerungs- und Telekommunikationssysteme“ in der geltenden Fassung zu verwenden.

L Risikoeinschätzung und Risikobehandlung (Risikomanagement)

Der Betreiber muss einen Prozess zum Risikomanagement der Netz- und Informationssystemsicherheit festlegen. Ziel dieses Prozesses ist es festzustellen, welche Risiken im Hinblick auf die Bereitstellung des wesentlichen Dienstes für die erfassten NIS-Assets bestehen und wie diese entsprechend zu behandeln sind.

Die allgemeinen Anforderungen an diesen Prozess sind in der ISO/IEC 27001 geregelt.

Bei der Ermittlung der Risiken für NIS-Assets, welche für die Bereitstellung des wesentlichen Dienstes notwendig sind, ist zu beachten, dass deren Sicherheit einerseits durch vorsätzliche Handlungen wie z. B. gezielte IT-Angriffe, Computer-Viren, Schadsoftware, Abhören und Manipulation der Kommunikation oder Diebstahl von Rechnern bedroht wird.

Andererseits sind bei der Risikoeinschätzung auch nicht vorsätzliche Gefährdungen insbesondere aus den folgenden Kategorien zu berücksichtigen:

- Elementare Gefährdungen,
- höhere Gewalt,
- organisatorische Mängel,
- menschliche Fehlhandlungen,
- technisches Versagen,
- Versagen oder Beeinträchtigung relevanter Infrastrukturen und externer Dienstleistungen,
- ungezielte Angriffe und Irrläufer von Schadsoftware.

Die Risikobehandlung umfasst die Auswahl angemessener Maßnahmen durch den Betreiber wesentlicher Dienste auf Basis der erfolgten Risikoeinschätzung. Bei der Beurteilung der Angemessenheit einer Maßnahme ist insbesondere deren technische und/oder organisatorische Umsetzbarkeit hinsichtlich ihrer Wirtschaftlichkeit zu berücksichtigen.

M Übertragung von Pflichten an Dienstleister

Wenn sich ein Betreiber im NIS-Scope Dienstleister bedient (z.B. zum Betrieb von Rechenzentren), dann sind die sich aus diesem 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 vertraglich festzulegen. Dessen ungeachtet verbleibt die Verantwortung beim Betreiber des wesentlichen Dienstes.

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

Anhang I. Übersichtstabelle Sicherheitsvorkehrungen in relevanten Dokumenten

Die Zuordnung auf die in diesem Dokument definierten, spezifischen Kapitel der in Kapitel E angeführten Standards können auf der von den Behörden betriebenen Anlaufstelle zum Netz- und Informationssystemsicherheitsgesetz und/oder der Webseite des Sektorenverbandes veröffentlicht werden.

Die folgende Tabelle 3 referenziert, in welchen Kapiteln des AT-3SV-Elektrizität die jeweiligen Sicherheitsmaßnahmen aus der Anlage 1 der NISV angesprochen werden.

Tabelle 3: Mapping Anlage 1 NISV mit AT-3SV-Elektrizität

Sicherheitsmaßnahmen iS Anlage 1 NISV	AT-3SV-Elektrizität (Technisch- und organisatorische Maßnahmen)
1. Governance und Risikomanagement	
1.1 Risikoanalyse	Kapitel K, L
1.2 Sicherheitsrichtlinie	Kapitel E
1.3 Überprüfungsplan der Netz- und Informationssysteme	Kapitel E, M
1.4 Ressourcenmanagement	Kapitel E, F
1.5 Informationssicherheitsmanagementsystemprüfung	Kapitel E
1.6 Personalwesen	Kapitel I
2. Umgang mit Dienstleistern, Lieferanten und Dritten	
2.1 Beziehungen mit Dienstleistern, Lieferanten und Dritten	Kapitel K, M
2.2 Leistungsvereinbarungen mit Dienstleistern und Lieferanten	Kapitel K
3. Sicherheitsarchitektur	
3.1 Systemkonfiguration	Kapitel E
3.2 Vermögenswerte	Kapitel F, I
3.3 Netzwerksegmentierung	Kapitel G
3.4 Netzwerksicherheit	Kapitel G
3.5 Kryptographie	Kapitel H, L
4. Systemadministration	
4.1 Administrative Zugangsrechte	Kapitel E
4.2 Systeme und Anwendungen zur Systemadministration	Kapitel F, I
5. Identitäts- und Zugriffsmanagement	
5.1 Identifikation und Authentifikation	Kapitel I
5.2 Autorisierung	Kapitel I
6. Systemwartung und Betrieb	
6.1 Systemwartung und Betrieb	Kapitel G, I
6.2 Fernzugriff	Kapitel G, I
7. Physische Sicherheit	
7.1 Physische Sicherheit	Kapitel I
8. Erkennung von Vorfällen	
8.1 Erkennung	Kapitel G, I
8.2 Protokollierung und Monitoring	Kapitel G, I
8.3 Korrelation und Analyse	Kapitel G, I
9. Bewältigung von Vorfällen	
9.1 Vorfallsreaktion	Kapitel E
9.2 Vorfallsmeldung	Kapitel E
9.3 Vorfallsanalyse	Kapitel E
10. Betriebskontinuität	
10.1 Betriebskontinuitätsmanagement	Kapitel L
10.2 Notfallmanagement	Kapitel L
11. Krisenmanagement	
11. Krisenmanagement	Kapitel I

Österreichs E-Wirtschaft

Brahmsplatz 3
1040 Wien

Tel +43 1 501 98-0
Fax +43 1 501 98-90 900

info@oesterreichsenergie.at
www.oesterreichsenergie.at

DVR 0422100, UID ATU37583307, ZVR 064107101; Raiffeisenlandesbank Niederösterreich-Wien AG, SWIFT/BIC: RLNWATWW, IBAN: AT12 3200 0000 1264 4787

Anhang II. Literaturverzeichnis

[1] *Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG).*

[2] Bundesminister für EU, Kunst, Kultur und Medien, *Verordnung zur Festlegung von Sicherheitsvorkehrungen und näheren Regelungen zu den Sektoren sowie zu Sicherheitsvorfällen nach dem Netz- und Informationssystemsicherheitsgesetz (Netz- und Informationssystemsicherheitsverordnung – NISV).*

[3] Österreichs E-Wirtschaft und Bundesverband der Energie- und Wasserwirtschaft, *Whitepaper Anforderungen an sichere Steuerungs- und Telekommunikationssysteme,* 2018.

[4] Bundeskanzleramt Österreich, *Österreichisches Informationssicherheitshandbuch,* 2016.