INFORMATIONSSICHERHEIT IN DER ENERGIEVERSORGUNG ANWENDUNG DES NETZINFORMATIONSSICHERHEIT- GESETZ

Oliver SKRBINJEK[1], Andreas STOCKNER[2], Manuel MESGEC[1], Georg ACHLEITNER[2]

Einleitung

Am 08.08.2016 wurde auf europäischer Ebene die Richtlinie 2016/1148 verabschiedet, die eine Vereinheitlichung des Sicherheitsniveaus in Branchen des öffentlichen Interesses innerhalb der Union adressiert. Mit dieser Richtlinie müssen alle Betreiber von wesentlichen Diensten ein definiertes Mindestmaß an Sicherheit erfüllen.

In Österreich wurde diese europäische Richtlinie am 05.02.2019 mit dem Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (NIS-G) umgesetzt. Ergänzend zum Gesetz wird in einer nationalen Richtlinie eine Festlegung getroffen welche Branchen davon betroffen sind und welcher Schwellwert innerhalb jeder einzelnen Branche als Grenzwert für die Anwendbarkeit gilt. Daher ist jeder Verteilernetzbetreiber, der den für ihn relevanten Schwellwert überschreitet, angehalten Maßnahmen zum Erreichen dieser Sicherheitsziele zu ergreifen.

An- und Herausforderungen

Das Gesetz wird durch weiterführende „Fact-Sheets“ ergänzt die dem betroffenen Netzbetreiber aufzeigen welche thematischen Schwerpunkte er in seine Betrachtung mit einbeziehen soll und grenzt diese, z.B. in ihrem Wirkungsbereich, auch ab. Im Wesentlichen werden die nachfolgenden Domänen adressiert:

- Governance and Ökosystem
- Absicherung von Schutz-, Automatisierungs- und Steuersystemen
- Verteidigung, Vorfallerkennung und Bewältigung von Vorfällen
- Resilienz

Viele Betreiber von wesentlichen Diensten haben bzw. hatten im Umfeld von Schutz-, Automatisierungs- oder Steuersystemen bis dato noch keine maßgeblichen Berührungspunkte mit der Informationssicherheit und bewegen sich hier auf „Neuland“. In Fachkreisen spricht man nicht in diesem Fall nicht mehr von IT-Security sondern von OT-Security (Operational Technologie).

Zusammenfassung

Grundsätzlich müssen die Anforderungen der Verfügbarkeit, der Integrität und der Vertraulichkeit der Systeme erfüllt bleiben. Für die Umsetzung müssen neue Systemfunktionen in bestehende Strukturen integriert und Bestandssysteme, sofern dies technisch möglich ist, adaptiert werden um erforderliche Schutzziele zu erreichen. Dies findet in allen Ebenen der Energieverteilung statt und verursacht, je nach angestrebtem Schutzziel und Ausprägung, erhebliche Investitions- und in Folge auch Systemwartungs-aufwände.

Im Beitrag werden Mindestschutzziele aufgezeigt sowie geeignete Methoden und Mechanismen für einen Lösungsansatz beschrieben und in ihrer Umsetzung den einzelnen Domänen (SCADA, Kommunikation, Anlage, zentrale Services) in ihrer Anwendung zugeordnet. Diese Zuordnung ermöglicht eine Abschätzung von Investitions- und Personalaufwendungen.

Der Beitrag zeigt auch auf, dass ein Umdenken erfolgen muss und nicht nur das Energieübertragungsnetz sondern auch ein dazugehöriges Datennetzwerk sicher zu betreiben ist.

[1] Energienetze Steiermark, Leonhardgürtel 10, 8010 Graz, oliver.skrbinjek@e-steiermark.com
[2] Austrian Power Grid AG, Wagramer Straße 19 (IZD-Tower), A-1220 Wien, andreas.stockner@apg.at