Bundesverband
Neue Energiewirtschaft e.V.
Hackescher Markt 4
D-10178 Berlin

Fon: +49 30 400548-0
mail@bne-online.de
www.bne-online.de

Rückmeldung zur öffentlichen Konsultation der

Cybersicherheitsverordnung 2

Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über die Agentur der Europäischen Union für Cybersicherheit (ENISA), den europäischen Rahmen für die Cybersicherheitszertifizierung und die Sicherheit der IKT-Lieferketten sowie zur Aufhebung der Verordnung (EU) 2019/881 (Cybersicherheitsverordnung 2)

Einordnung

Die von der EU-Kommission vorgeschlagene Cybersicherheitsverordnung 2 erfasst die Risiken von IKT-Lieferketten, die unter anderem fernsteuerbare elektrischen Anlagen mit potenzieller Relevanz für kritische Infrastrukturen betreffen. Wir möchten voranstellen, dass wir grundsätzlich technische gegenüber regulatorischen Lösungsansätzen priorisieren. Jede Form von regulatorischen Vorgaben geht unweigerlich mit technischen und ökonomischen Folgerisiken einher. Lediglich in spezifischen Bereichen mit besonders hohen Sicherheitsanforderungen halten wir ordnungspolitische Maßnahmen für sinnvoll.

Generelle, absolute Ausschlüsse bestimmter Hersteller (Unternehmen oder aufgrund von Herkunftsland) stellen ein erhebliches operationelles Risiko dar. Sowohl die Stabilität des Netzbetriebs als auch die Servicequalität könnten durch notwendig werdende aufwendige, zeitlich eng getaktete Migrationsprojekte unter Druck geraten. Derartige Vorhaben sind typischerweise anfällig für Betriebsunterbrechungen, Leistungseinbußen und Verzögerungen – insbesondere, wenn bestehende Infrastruktur in großem Maßstab ausgetauscht werden müsste. Vorrang sollten stattdessen technische Schutzmaßnahmen haben, etwa Zugriffssteuerung, Netzwerksegmentierung oder die Limitierung bidirektionaler Kommunikationsverbindungen.

Bei der Bewertung der Cybersicherheitsrisiken erachten wir es als wichtig, dass zwischen gewerblich betriebenen Kraftwerken (Utility-Scale-Solarkraftwerken und -Batteriespeichersystemen (BESS)), Commercial & Industrial (C&I) Anlagen und dezentralen kleineren Energiewende-Anlagen (Gebäude-PV, nichtöffentliche Ladepunkte, Wallboxen, Heimbatteriespeicher, Wärmepumpen) unterschieden wird. Zwischen diesen unterschiedlichen Anlagentypen bestehen erhebliche Unterschiede bei den Anforderungen zur sicheren IT-Anbindung und Abwehr möglicher Cybersicherheits-Angriffe. Große Anlagen werden professionell mit IT- und Sicherheitstechnik angebunden, abgeschirmt und regelmäßigen (Sicherheits-)Updates und Überprüfungen der Kommunikationsstrecke unterzogen, da die Verfügbarkeit der Anlagen hohen monetären Auswirkungen unterliegt. Kleinere Anlagen hingegen nutzen zur Kommunikation z.B. mit cloudbasierten Backend-Anwendungen oft private Internetverbindungen, weshalb moderne IKT-Konzepte nötig sind, um Risiken zu minimieren.

I. IT-Sicherheit bei Utility-Scale-Solarkraftwerken/-BESS[1]

Für diese Anlagentypen besteht die IT-Anbindung aus Netzwerk-Firewalls, VPN-Gateways, verschlüsselten Datenloggern und operativen Sicherheitskontrollen, um die Anlagen vor digitalen Angriffspfaden zu schützen.

- Wechselrichter und sonstige Anlagenkomponenten werden kommunikationstechnisch separiert und vom Internet getrennt betrieben. Die Anlagen sind vom öffentlichen Kommunikationsnetz oder den Hersteller-Clouds getrennt.

[1] Abgrenzungsvorschlag bzgl. der elektrischen Leistung: Gemeint sind Anlagen die ein elektrotechnisches Anlagenzertifikat Typ A nach VDE-AR-N 4120 benötigen (also > 950 kW): Dieser Leistungswert ergibt sich aus EU Network Code Requirements for Generators (RfG).

- Sämtliche IT-Komponenten der Anlagen- und Steuerungstechnik sind innerhalb des Betreiber-Netzwerks isoliert und segmentiert, wodurch sie wirksam vor externen Zugriffen geschützt werden.
- Jede Anlage (z.B. ein Solarpark) ist über einen verschlüsselten, authentifizierten Kanal (z.B. in Deutschland nach BSI TR-02102-x[2]) sicher in eine zentrale Infrastruktur eingebunden und nicht aus dem Internet erreichbar. Auch lassen sich moderne sichere Alternativen zu VPN-Kanälen umsetzen.
- Die IT-Netzwerke der Unternehmen sind von der OT-Infrastruktur der Anlagen durch Firewalls separiert.

Die Herkunft einzelner Hardware-Komponenten begründet keinen allgemeinen Fernzugriff, weil es sichere IT-Setups über Steuerung, Software-Updates und Zugriffsrechte gibt. Die zentrale Anlagensteuerung erfolgt ausschließlich über Modbus[3], Datenloggern und SCADA-Systemen mit individuellen Zugangsdaten. Jeder Zugriff erfolgt über eine abgesicherte VPN-Verbindung. Ein externer Akteur – einschließlich des Wechselrichterherstellers – kann weder Daten abfragen noch Anlagen unbemerkt steuern oder gar außer Betrieb setzen.

II. IT-Sicherheit bei C&I -Solaranlagen/-BESS[4]

Bei C&I-Anlagen handelt es sich ebenfalls meist um größere Anlagen, die in der Regel direkt Unternehmen mit Energie versorgen (z.B. die PV-Anlage auf der Industriehalle oder Ladeinfrastruktur auf Firmenparkplatz) und erhöhte Sorgfalt bei der IT erfordern. Sind C&I-Anlagen z.B. direkt mit Energiemanagementsystemen der Unternehmen verbunden, wird die IT-Verbindung ebenfalls abgesichert (z.B. in Unternehmensnetzwerken). Diese Kommunikationsanbindungen schützt das versorgte Unternehmen im Rahmen seiner IT-Strategie gegen unautorisierte Zugriffe von außen.

III. IT-Sicherheit bei dezentralen Kleinanlagen, (i.d.R. Betrieb durch Privatpersonen)

Im Gegensatz zu Utility-Scale-Solarkraftwerken/-BESS oder C&I-Anlagen kommunizieren dezentrale Kleinanlagen überwiegend direkt mit Cloud-Plattformen. Die verbauten Wechselrichter sind zumeist mit den Hersteller-Cloud-Systemen verbunden: Steuerung, Monitoring und Software-Updates erfolgen über Hersteller-Apps sowie externe Server, die aktuell mehrheitlich in der EU verortet sind. Die Anlagen haben keine physikalisch getrennten IT-Systeme und sind meistens in das LAN/WLAN der Privatpersonen eingebunden. Cloudverbindungen bestehen ggf. auch zu Serviceanbietern von Home-Energy-Management-Systemen (HEMS) und/oder Direktvermarktern, wobei gängige Authentifizierungsmaßnahmen Standard sind (Passwortschutz, TLS). In Deutschland besteht zusätzlich eine sicher Kommunikationsstrecke über ein BSI-zertifiziertes intelligentes Messsystem (iMSys) und ggf. einer zertifizierten Steuerbox (sofern vorhanden).

[2] VPN-Router nach BSI TR-02102 sind weiterhin der Standard für klassische Site-to-Site-Verbindungen. (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zulassung/VS-Anforderungsprofile/BSI-VS-AP-0001.pdf?__blob=publicationFile&v=3). Für den Remote-Zugriff (Client-to-Site) kommen auch zunehmend ZTNA/SASE-Lösungen in Anwendung, da diese sicherer und flexibler sind.

[3] Modbus über VPN ermöglicht den sicheren Fernzugriff auf Modbus TCP/RTU-Geräte (z.B. Wechselrichter, SPS) über das Internet, indem ein verschlüsselter Tunnel (VPN) zwischen Client und Anlage genutzt wird. Dies ersetzt unsicheres Port-Forwarding, wobei die Verbindung idealerweise über VPN-Router oder Gateways (z.B. OpenVPN) erfolgt.

[4] Abgrenzungsvorschlag bzgl. der elektrischen Leistung: Gemeint sind Anlagen, die ein elektrotechnisches Anlagenzertifikat Typ B nach VDE-AR-N 4110benötigen (135 kW – 950 kW).

Empfehlungen

Die Strategie der EU sollte daraufsetzen, die Wettbewerbsfähigkeit und den Klimaschutz Europas, insbesondere bei Schlüssel- und Zukunftstechnologien durch geeignete industriepolitische Maßnahmen und den Anschub lokaler Produktion zu stärken. Für diese leisten nicht-europäische Zulieferer und Hersteller im Bereich der Erneuerbaren Energien einen wichtigen Beitrag.
Eine gesteuerte, an Risikokriterien orientierte Einbindung unterschiedlicher Anbieter mit bewusst breiter Herstellervielfalt, kann ein robustes Sicherheitsniveau gewährleisten. Maßnahmen wie durchgängige Verschlüsselung, unabhängige Code-Prüfungen, Zertifizierungsprozesse und verbindlich festgelegte Serviceanforderungen reduzieren Risiken effektiv – ohne dabei die Resilienz der kritischen Infrastruktur zu schwächen.

Der bne rät davon ab, bestimmte Länder zu Hochrisikoländern zu erklären und schlägt stattdessen vor, folgende Sicherheitsgrundsätze für den ganzen Markt und die Zulieferketten anzuwenden:

1. Cybersicherheit: Risiken richtig bewerten

Risikobewertungen sollten für **alle Hersteller** anhand einer möglichen Gefährdung der Energieversorgung erfolgen: Hierbei wird gefragt, inwiefern die eigene Anlage aufgrund von Vernetzung, Zentralisierung und einheitlicher Betriebsverfahren die Energieversorgung gefährden könnte und welche Maßnahmen im Falle eines Angriffs vorgenommen werden. **Es ist dabei dringend zu differenzieren zwischen professionell betriebenen Großanlagen, C&I-Anlagen und dezentralen Kleinanlagen von Privatpersonen.** Für Großanlagen sollten andere Maßstäbe gelten als für Kleinanlagen.
Die **Risikobewertung kann nicht allein auf Basis einer Komponentenbetrachtung erfolgen**, sondern muss jeweils die konkreten, technischen Elemente und Anwendungsfälle betrachten. Am Ende zählt nicht nur, ob einzelne Komponenten der Anlagen sicher sind, sondern wie sicher das Anlagensystem insgesamt ist.

2. Bürokratieabbau: Zertifizierung vereinheitlichen und anerkennen

Der CSA 2 hat mit ENISA die Chance, die Komplexität bei der Zertifizierung zu reduzieren. Einerseits durch die Einführung von europaweit einheitlichen Zertifikaten und andrerseits durch **die gegenseitige Anerkennung und Leistungsfähigkeitsabgleich von nationalen wie internationalen Zertifikatsverfahren.** Dadurch können derzeitige widersprüchliche Zertifizierungsstandards durch teilweise konträr verlaufende europäische und mitgliedsstaatenspezifische Vorgaben aufgelöst werden. Eine allgemeine, europaweit gültige Compliance ist zu begrüßen.

3. Verantwortung für die Cybersicherheit

Bei Utility-Scale-Solarkraftwerken/-BESS kann und muss die Verantwortung für die Anlage und die Verfügbarkeit von Stromkapazität der Anlagenbetreiber tragen. Bei dezentralen Kleinanlagen von Privatpersonen hingegen muss die Verantwortung für die IT-Sicherheit beim Anlagenhersteller verortet sein (Security by Design), da Privatpersonen nicht für die Cybersicherheit der Anlagen verantwortlich gemacht werden können.

4. Anforderungen an Cybersicherheit differenzieren

Das Sicherheitsniveau im Bereich der dezentralen Kleinanlagen entspricht nicht dem von Utility-Scale-Solarkraftanlagen/-BESS und C&I-Anlagen und dieses Sicherheitsniveau ist auf Anlagenebene auch nicht anzustreben. Gewerblich betriebene Großanlagen haben getrennte IT-Systeme (s.o.). Bei Großanlagen wird bereits heute der unbefugte externe Zugriff technisch verhindert[5]. Kleinanlagen sind in IT-Netzwerke von Privatpersonen eingebunden und überwiegend mit der Cloud der Hersteller oder mit Systemen der Versorger (z.B. Backendsysteme von Portalen und mobile Apps oder mit HEMS) verbunden. Statt auf pauschale Verbote, sollte der Fokus auf dem Aufbau von Resilienz und einer bewussten Bewertung von Cloud-Anbindungen liegen. Zudem sollte berücksichtig werden, dass gerade bei Kleinanlagen die regulierten und zertifizierten Messsysteme (Smart-Meter, in Deutschland iMSys und Steuerboxen) sichere Messwertübertragung und sichere Kommunikationskanäle bereitstellen können.

5. Update-Pflicht für Software von dezentrale, kleine Energiewendeanlagen

Bei gewerblich betriebenen Anlagen schützt die IT-Infrastruktur vor unautorisierter Kommunikation. Bei Anlagen von Privatpersonen ist es deutlich schwieriger, dauerhaft ein angemessenes Sicherheitsniveau sicherzustellen. Das zentrale Risiko besteht weniger darin, dass Software vollständig fehlerfrei sein müsste - das ist praktisch unmöglich -, sondern darin, dass bekannt gewordene Sicherheitslücken oder Softwarefehler nicht zeitnah behoben werden. Entscheidend ist daher nicht nur, dass Hersteller Fehlerkorrekturen bereitstellen, sondern auch, dass diese Updates schnell, zuverlässig und möglichst flächendeckend auf die betroffenen Geräte ausgerollt werden, einschließlich älterer Geräte, die weiterhin in Betrieb sind.
Besonders wichtig ist deshalb eine verbindliche Update-Pflicht für Hersteller. Sie muss auch Fälle berücksichtigen, in denen ein Hersteller insolvent wird oder ein Produkt abkündigt. Andernfalls besteht das Risiko, dass zahlreiche Anlagen mangels Sicherheitsupdates außer Betrieb genommen werden müssten. Um dies zu vermeiden, sollten klare Verpflichtungen geschaffen werden:

a. Privatpersonen sollten für das Energiesystem kritische Anlagen nur betreiben, wenn Software-Updates über die Lebensdauer der Anlage sichergestellt sind. Hersteller müssen hierfür geeignete Vorkehrungen treffen, um die Updatefähigkeit und sichere Wartung dauerhaft zu gewährleisten, auch für den Fall, dass der ursprüngliche Support (z.B. durch Insolvenz des Herstellers) nicht mehr erbracht werden kann. Als eine mögliche Option kann – soweit technisch und sicherheitsarchitektonisch vertretbar – auch eine Hinterlegung relevanter Softwarebestandteile bei einer neutralen Stelle (in Deutschland etwa dem BSI) in Betracht kommen (= Escrow). Ziel ist es, dass bei Wegfall des Herstellersupports eine sichere Weiterwartung ermöglicht wird und Privatpersonen ihre Anlage möglichst ohne unverhältnismäßige Hürden an ein anderes Backend oder HEMS anbinden können.
b. Im Sinne des Verbraucherschutzes wäre es sinnvoll, wenn proprietäre (= herstellerspezifische) Kommunikationsprotokolle zwischen Anlage und Backend offengelegt würden, sodass Privatpersonen einen anderen Backend-Anbieter wählen können. Das kommt einem Unbundling von Anlage und den Services gleich.
c. Für größere Anlagenpools braucht es höhere Anforderungen. Daher sollten für kleine Anlagen unterschiedliche Risikoklassen definiert werden, die sich mit der aggregierten Leistung der Anlagenpools in ihren Cybersicherheits-Anforderungen erhöhen (z.B. Backend mit insgesamt verbundenen Anlagen < 1 GW → Klasse I mit Konformitätserklärung durch den Hersteller, darüber Klasse II mit Konformitätsbewertung etc.).

[5] gesetzlich verpflichtende Zugriffe staatlicher Stellen können jedoch nicht grundsätzlich ausgeschlossen werden

6. Planbarkeit für die Investoren verbessern

In Artikel 100 geht es um die Benennung von Drittländern, die zu Hochrisikoländern erklärt werden (könnten): Um Investitionssicherheit und Bestandsschutz zu gewährleisten, sowie abrupte Betriebs- oder Bauunterbrechungen bei laufenden und geplanten Solar- und BESS-Projekten zu vermeiden, ist es wichtig zu beachten, dass bereits erteilte Zertifikate nicht ihre Gültigkeit verlieren sollten.

Fazit: Keine Vermischung von Cybersicherheit und Handelspolitik

Die regulatorischen Anforderungen der EU-Kommission im Rahmen der Gesetzesinitiative Cybersicherheitsverordnung 2 sollten sich an der IT-/OT-Architektur und der Steuerbarkeit von Energiewendeanlagen orientieren, nicht an der Erzeugungstechnologie oder der Herkunft einzelner Komponenten. Pauschale Einschränkungen bringen keinen Sicherheitsgewinn, einheitliche Produktsicherheitszertifizierungen hingegen schon.