Vom Messpunkt zum Steuerpunkt: Die neue Angriffsfläche der Verteilnetze

Arthur Raess

Mit der Neufassung des § 14a Energiewirtschaftsgesetz (EnWG) und dem Hochlauf intelligenter Messsysteme wird der Netzanschluss vom Messpunkt zum Steuerpunkt: Digitale Befehle greifen in den physischen Netzbetrieb ein. Die Angriffsfläche, die dabei entsteht, liegt weniger im zertifizierten Smart-Meter-Gateway als in der Systemlandschaft dahinter, von den Backends der Marktrollen bis zur Rundsteuertechnik im Bestand. Das NIS-2-Umsetzungsrecht verlangt inzwischen den fortlaufenden Nachweis wirksamer Maßnahmen. Mit jährlichen Penetrationstests ist dieser Anspruch nicht einzulösen.

Wer bisher Zählerdaten manipulierte, verfälschte eine Abrechnung. Wer künftig Steuerkanäle manipuliert, greift in den physischen Netzbetrieb ein. Zwischen diesen beiden Sätzen liegt die sicherheitsarchitektonische Zäsur, die der § 14a EnWG für die Verteilnetze bedeutet. Die öffentliche Debatte um den Rollout kreist um Tempo, Kosten und Marktrollenkomplexität; die Frage, wie sich eine steuerbar gewordene Netzebene fortlaufend gegen Angriffe validieren lässt, bleibt dagegen unterbelichtet. Dabei stammen die Prüfverfahren, mit denen Netzbetreiber ihre Systeme heute absichern, aus der Zeit vor dieser Verschiebung.

Im steuerbaren Verteilnetz ist jeder Kanal Betriebsmittel und Angriffsfläche zugleich *Bild: Adobe Stock*

Aus Lesen wird Schreiben

Seit dem 1. Januar 2024 müssen neue steuerbare Verbrauchseinrichtungen mit mehr als 4,2 kW Bezugsleistung, also Wärmepumpen, private Ladepunkte, Klimageräte und Speicher, vom Verteilnetzbetreiber netzorientiert gedimmt werden können. Das Verfahren definiert die Festlegung BK6-22-300 der Bundesnetzagentur. Im Zielbild erzeugt das System des Netzbetreibers den Befehl. Transportiert wird er durch einen vom Gateway-Administrator eingerichteten, TLS-gesicherten und über Zertifikate der Smart-Metering-PKI beidseitig authentisierten Kanal zum Smart-Meter-Gateway. Dort wird er über die CLS-Schnittstelle an eine Steuerbox durchgereicht, und erst deren EEBus-, Modbus- oder SG-Ready-Abgang übersetzt ihn in eine tatsächliche Leistungsreduktion. Ein einziger Dimmbefehl durchquert damit mehrere Marktrollen, zwei Zertifizierungsregime und mindestens drei Protokollwelten, bevor er ein Relais bewegt.

Produktive Realität ist dieser Pfad erst in Ansätzen. Viele Netzbetreiber steuern übergangsweise präventiv über statische Zeitfenster. Die netzorientierte Steuerung setzt eine belastbare Netzzustandsermittlung voraus, die vielerorts erst aufgebaut wird, und CLS-Kanäle sind bei etlichen Messstellenbetreibern nicht produktiv geschaltet. Regulatorisch aber ist die Richtung fixiert: Die Übergangsregelungen laufen Ende 2028 aus, und mit jedem Rollout-Quartal wächst die Zahl der Anschlusspunkte, an denen ein digitaler Befehl eine physische Last schaltet.

Der Charakter des Anschlusspunkts ändert sich damit grundlegend. Ein digitaler Zähler kann als ggf. kompromittierter Sensor falsche Daten liefern, was abrechnungsrelevant wird, netzbetrieblich aber beherrschbar ist. Bedenklicher wird es, wenn der Steuerpunkt als Aktor fungiert, denn ein kompromittierter Aktor kann fremde Befehle ausführen. Die Vertraulichkeit der Messwerte bleibt Schutzziel, verliert aber ihren Rang. Maßgeblich sind jetzt Integrität und Verfügbarkeit des Steuerkanals.

Die Kette hinter dem Gateway

Reflexhaft richtet sich dann der Blick auf das Smart-Meter-Gateway (SMGW). Das greift zu kurz. Zertifiziert nach Common Criteria gegen ein eigenes Schutzprofil und konform zur Technischen Richtlinie BSI TR-03109, mit Sicherheitsmodul, definierten Kommunikationsprofilen und eigener Public-Key-Infrastruktur (PKI) als Vertrauensanker, ist das SMGW bei aller Kritik an Rollout-Tempo und Komplexität das am besten geprüfte Einzelgerät der gesamten Kette.

Die Angriffsfläche entsteht um das Gateway herum. Steuerboxen am CLS-Kanal durchlaufen zwar eine Prüfung nach TR-03109-5, doch dahinter beginnt eine

andere Welt: EEBus, Modbus und Smart-Grid-Ready-Kontakte wurden für Interoperabilität entworfen. Und die herstellereigenen Schnittstellen der Energiemanagementsysteme entziehen sich jeder einheitlichen Prüfung. Hinzu kommen die Backends der Marktrollen, die Steuerbefehle erzeugen, signieren und verteilen: Gateway-Administration, aktive externe Marktteilnehmer bzw. Steuerplattformen der Netzbetreiber. Wer eines dieser Systeme kontrolliert, braucht kein einziges Gateway zu brechen. Er nutzt die legitime Infrastruktur mit.

Dazu kommt die Bestandswelt, die im Diskurs um intelligente Messsysteme regelmäßig unterschlagen wird. Ihre Verwundbarkeit ist keine Vermutung: Ende 2024 wiesen die Sicherheitsforscher Fabian Bräunlein und Luca Melette nach, dass sich die unverschlüsselten Langwellensignale der Funkrundsteuerung im jahrzehntealten Versacom-Protokoll fälschen lassen, inklusive der Möglichkeit, mit einer einzigen Nachricht sämtliche Empfänger eines Energieversorgers zu adressieren. Nach ihrer Schätzung hängen rund 40 der 250 GW installierter Leistung in Deutschland an dieser Technik.

Ähnliches gilt für die Fernwirktechnik der Ortsnetzstationen: IEC 60870-5-104 transportiert Befehle in der Fläche unverschlüsselt, die Härtung nach IEC 62351 bleibt die Ausnahme. Fernwartungszugänge von Komponentenherstellern und Dienstleistern sowie historisch gewachsene Kopplungen zwischen Leitsystem und Büro-IT vervollständigen das Bild. Die neue Steuerarchitektur ersetzt diese Welt nicht, sie kommt hinzu. Ein Verteilnetzbetreiber betreibt 2026 mehrere Generationen von Steuertechnik parallel, jede mit eigenen Schwachstellen, Zuständigkeiten und Dienstleistern.

Sicherheitsarchitektonisch gilt der Satz von der Kette und ihrem schwächsten Glied. Nur reicht die Kette hier von der Festlegung der Bundesnetzagentur bis zum Relaiskontakt im Zählerschrank, und an fast jedem Glied trägt ein anderer Akteur die Verantwortung.

Das Aggregationsrisiko

Als Einzelziel ist die Wärmepumpe uninteressant; ihre Manipulation erzeugt einen unzufriedenen Kunden, kein Netzproblem. Relevant wird die Steuerbarkeit durch Aggregation, und zwar konstruktionsbedingt: Steuerbare Verbrauchseinrichtungen sind genau dafür ausgelegt, in großer Zahl koordiniert geschaltet zu werden.

Die Größenordnungen sind schnell hergeleitet. Der Referenzstörfall, auf den die Primärregelreserve des kontinentaleuropäischen Verbundnetzes dimensioniert ist, beträgt 3.000 MW. Eine Million koordiniert schaltbarer Anschlüsse, an denen sich im Mittel nur 3 kW gleichzeitig bewegen lassen, erreicht diese Marke. Bei 11-kW-Ladepunkten genügt ein Bruchteil davon. Unter dem Schlagwort MadIoT haben Soltan, Mittal und Poor (USENIX Security 2018) gezeigt, wie synchrone Schaltvorgänge einer solchen Last Frequenz- und Spannungshaltung unter Druck setzen und im Extremfall Schutzauslösungen provozieren. Für das Szenario muss ein Angreifer keine hunderttausend Geräte einzeln kompromittieren. Es genügt der Zugriff auf eine Stelle, die viele Geräte legitim ansteuert: eine Steuerplattform, eine Update-Infrastruktur, ein Hersteller-Backend, ein Dienstleister mit weitreichenden Fernwartungsrechten.

Welche Reichweite solche zentralen Kanäle haben, zeigte der 24. Februar 2022. Der Wiper-Angriff auf das Satellitennetz KA-SAT galt der ukrainischen Kommunikation; als Kollateralschaden verloren rund 5.800 Windenergieanlagen in Deutschland ihre Fernüberwachung und Fernwartung. Die Anlagen liefen weiter, die Betreiber kamen wochenlang nicht an sie heran. Angegriffen hatte diese Anlagen niemand. Es reichte, dass ihr Steuerkanal über eine Infrastruktur lief, die ein Dritter zerstörte.

Das lohnende Angriffsziel wandert damit nach oben in der Architektur: nicht der Zählerschrank zählt, sondern die Systeme, die Zählerschränke in Masse erreichen. Diese Systeme sind klassische IT, mit allem, was dazugehört: Identitäten, Schnittstellen, Cloud-Diensten und Softwarelieferketten. Die vielzitierte IT/OT-Konvergenz ist im Verteilnetz keine Zukunftsdiagnose mehr, sondern die Beschreibung des Ist-Zustands. Mit der Besonderheit, dass am Ende der IT-Kette keine Datenbank steht, sondern ein Netzgebiet.

Ein Prüfregime aus einer anderen Zeit

Dem steht ein Prüfregime gegenüber, das im Kern auf der Momentaufnahme beruht. Der turnusmäßige Penetrationstest, jährlich oder im Zertifizierungszyklus, prüft einen definierten Scope zu einem definierten Zeitpunkt. Das war angemessen, solange sich die geprüfte Umgebung zwischen zwei Prüfungen kaum veränderte.

Genau diese Voraussetzung ist im digitalisierten Verteilnetz entfallen. Relevant sind neue Gerätegenerationen und Firmwarestände, neue Marktrollen- und Dienstleisterbeziehungen, die Migration von präventiver zu netzorientierter Steuerung, produktiv geschaltete CLS-Kanäle sowie die wachsende Kopplung mit Flexibilitätsplattformen. Ein Prüfbericht vom Frühjahr beschreibt im Herbst eine Infrastruktur, die es so nicht mehr gibt.

Hinzu kommt ein strukturelles Problem, das jeder kennt, der solche Tests beauftragt oder durchgeführt hat: Im Kick-off fällt verlässlich der Satz, die Leittechnik bleibe aus dem Scope. Die Sorge um den laufenden Betrieb ist berechtigt. Das Ergebnis hat dann aber einen blinden Fleck exakt dort, wo die Konsequenzen eines Angriffs am größten wären. Geprüft wird, was risikolos prüfbar ist, nicht, was geprüft werden müsste.

Der regulatorische Rahmen hat den Anspruch inzwischen nachgezogen. Seit dem 6. Dezember 2025 ist das NIS-2-Umsetzungsgesetz in Kraft. Für den Energiesektor verankert der Gesetzgeber die verschärften Anforderungen an Risikomanagement und Meldewesen nicht im BSI-Gesetz, sondern unmittelbar im Energiewirtschaftsgesetz (EnWG). Die neuen §§ 5c bis 5e treten an die Stelle des bisherigen § 11. Den Maßstab konkretisiert die Bundesnetzagentur im Einvernehmen mit dem BSI in einem überarbeiteten IT-Sicherheitskatalog. Bis zu dessen Veröffentlichung gelten die bestehenden Kataloge fort. Bemerkenswert ist weniger der erweiterte Adressatenkreis als die inhaltliche Akzentverschiebung: Verlangt ist nicht der Nachweis, dass irgendwann geprüft wurde, sondern die fortlaufende Bewertung der Wirksamkeit der getroffenen Maßnahmen. Wirksamkeit ist keine

Eigenschaft, die man einmal jährlich feststellt. Sie ist ein Zustand, der sich mit jeder Änderung der Umgebung neu beweisen muss.

Kontinuierliche Validierung in der OT-Realität

Wie lässt sich dieser Anspruch einlösen, ohne den Netzbetrieb zu gefährden? Aus unserer Prüfpraxis in KRITIS-Umgebungen haben sich Prinzipien herausgebildet, die weniger eine Frage des Werkzeugs sind als der Methodik.

1. Angreiferperspektive als Ausgangspunkt: Angreifer priorisieren nach Erreichbarkeit, nicht nach Common Vulnerability Scoring System (CVSS). Relevant ist deshalb nicht die vollständige Liste theoretischer Schwachstellen, sondern die Frage, welche Pfade von außen, über Internet-exponierte Systeme, Dienstleisterzugänge, Fernwartung oder die Büro-IT, tatsächlich bis an steuerungsrelevante Systeme heranführen. Eine mittelschwere Schwachstelle auf einem erreichbaren Sprungsystem wiegt schwerer als eine kritische Lücke tief in einer sauber getrennten Zone.
2. Übergänge als eigentlicher Prüfgegenstand: Die zentrale Sicherheitsleistung eines Verteilnetzbetreibers ist die Trennung der Zonen, zwischen Büro-IT und Leittechnik, zwischen Marktkommunikation und Steuerkanal, zwischen Dienstleisterzugang und Prozessnetz. Netzpläne dokumentieren den Soll-Zustand, Angreifer arbeiten mit dem Ist-Zustand. Segmentierung bleibt eine Behauptung, solange sie nicht regelmäßig aus der Angreiferposition verifiziert wird, und zwar erneut nach jeder Firewall-Änderung, jedem neuen Dienstleister, jedem Systemwechsel.
3. Abgestufte Eingriffstiefe statt pauschaler Schonung: In produktiven Prozessnetzen haben aggressive Scans nichts verloren; dort sind passive Verfahren, Konfigurations- und Architekturanalysen das Mittel der Wahl. Aktive, tiefe Prüfungen gehören in Referenz- und Staging-Umgebungen sowie an die definierten IT/OT-Schnittstellen. Wer diese Abstufung sauber konzipiert, prüft kontinuierlich, ohne den Betrieb zu berühren, und muss die Leittechnik nicht länger aus dem Scope streichen.
4. Wiederholbarkeit als Nachweisinstrument: Der Wert kontinuierlicher Validierung liegt nicht im einzelnen Befund, sondern in der Zeitreihe. Erst die wiederholte Prüfung zeigt, ob eine behobene Schwachstelle geschlossen bleibt, ob eine Änderung neue Pfade geöffnet hat und ob sich die Lage verbessert oder nur verschiebt. Gegenüber Auditoren und Aufsicht ist eine lückenlose Zeitreihe ein qualitativ anderes Fundament als ein achtzehn Monate alter Bericht.
5. Prüfinfrastruktur als eigenes Schutzobjekt. Wer kontinuierlich validiert, erzeugt fortlaufend hochsensible Daten: Netzarchitekturen, Schwachstellen, Zugangspfade in kritische Infrastruktur. Verteilnetzbetreiber sollten deshalb prüfen, wo Prüfplattformen betrieben werden und welchem Rechtsrahmen ihre Anbieter unterliegen. Telemetrie über Angriffsflächen deutscher Netze gehört nicht in Jurisdiktionen, deren Behörden sich per Gesetz Zugriff verschaffen können; der amerikanische CLOUD Act ist nur das bekannteste Beispiel.

Der Steuerpunkt bleibt

Über das Tempo des Rollouts lässt sich streiten, über die Komplexität der Marktrollen ebenso, und auch darüber, wann netzorientierte Steuerung flächendeckend gelebte Praxis wird. Nicht streiten lässt sich über die Richtung. Die Verteilnetze werden steuerbar, über digitale Kanäle, die von der Festlegung der Bundesnetzagentur bis zum Relaiskontakt reichen. Jeder dieser Kanäle ist Betriebsmittel und Angriffsfläche zugleich.

Für die Sicherheitsorganisation folgt daraus etwas Unbequemes. Die Prüfkadenz muss der Änderungskadenz der Infrastruktur folgen. Eine Umgebung im Dauerumbau lässt sich nicht mit jährlichen Momentaufnahmen absichern. Verteilnetzbetreiber, die den Übergang vom Messpunkt zum Steuerpunkt vollziehen, sollten denselben Übergang in ihrer Sicherheitsvalidierung nachvollziehen: von der Prüfung als Ereignis zur Prüfung als Betriebszustand. Das Netz von morgen wird kontinuierlich gesteuert. Es sollte auch kontinuierlich geprüft werden.

A. Raess, Geschäftsführer, VORNAC GmbH, Heidelberg
arthur@vornac.com