Broschüre

Cybersicherheit für die deutsche Energiewirtschaft

Erzeuger, Verteilnetzbetreiber und Stadtwerke.

Die digitale Energiewende mit Fortinet sichern

Die deutsche Energiewende entwickelte sich aus den folgenden Faktoren heraus: Ausstieg aus der Atom- und Kohleenergie, Transformation in ein nachhaltiges Energiesystem sowie Dezentralisierung und Liberalisierung des Energiemarktes. Dieser Wandel stellt die Absicherung der Energieinfrastrukturen vor Cyberangriffen vor völlig neue Herausforderungen.

Cybersicherheit für Energieinfrastrukturen

Die Substitution großer Kraftwerke durch eine hohe Anzahl dezentraler Einspeisung erneuerbarer Energien – u.a. Wind, Wasser, Sonne – führt zu wesentlich höheren Anforderungen an die Netzsteuerung, um die Stabilität des Stromnetzes zu gewährleisten.

Durch diese Dezentralisierung steigt gleichzeitig das Risiko von Cyberbedrohungen für die Infrastruktur an, da im Vergleich zu Großkraftwerken der physische Schutz verteilter Steuerungssysteme deutlich schwieriger ist.

Zusätzlich zu bedarfsgerechter Steuerung von Energieeinspeisung in die Netze muss das, typischerweise bei erneuerbaren Energien, kontinuierlich wechselnde Energieangebot nachgeregelt werden. Die Bundesnetzagentur senkt, angepasst an den steigenden Energieanteil erneuerbarer Energien, fortlaufend die Leistungsgrenze, welche die ungeregelte Einspeisung in das Netz festlegt. Im Zuge der Transition von fossilen hin zu erneuerbaren Energieträgern steigt somit auch der Bedarf an aktiver Steuerung im Feld. Stabile und störungsfreie Steuerungen für die Netzstabilität sind daher unerlässlich.

Mit dem Ausbau der typischerweise über öffentliche IP-Netze angebundener Steuerungstechnik wächst im gleichen Maße die Angriffsfläche auf die Steuerungsnetze der Energieversorger und damit das Risiko auf die Versorgungssicherheit infolge der Energiewende.

Herausforderungen auf einen Blick

- Die deutsche Energiewende stellt die Energieerzeugung, -verteilung und auch die Cybersicherheit vor neue Herausforderungen.
- Der Bedarf an aktiver Steuerung des Netzes steigt stetig, um Netzstabilität zu gewährleisten.
- Dezentralisierung und Liberalisierung führen zur Erweiterung der Angriffsfläche.
- Der Wandel von geschlossenen zu offenen Netzen bietet weitere Einfallstore für Cyberangriffe.

Netzwerk- und Informationssicherheit sind das Gebot der Stunde, insbesondere für die kritische Infrastruktur wie Energienetze

Aus den genannten Entwicklungen am Energiemarkt wird eine verschlüsselte Kommunikation über ein zuverlässiges VPN-Netz benötigt. Um dieses über das öffentliche Netz eines Providers zu gewährleisten, kommen VPN-Konzentratoren zum Einsatz. Die Außenstellen werden, je nach vorliegenden örtlichen Gegebenheiten, mit einem speziellen Industrie-Hutschienen- oder einem Standard-Gerät ausgestattet. Dieses dient einerseits zur Anbindung an die VPN-Gegenstelle in der Zentrale und anderseits dafür, bereits vor Ort gegen mögliche Cyberattacken zu filtern. Ebenfalls darf die Tatsache nicht außer Acht gelassen werden, dass Kriminelle physisch einen Schaltschrank aufbrechen können und daher eine Filterung der Kommunikation und Protokolle innerhalb des Netzes nötig ist.

Was ist notwendig, um diese Infrastrukturen zu schützen?

Wesentlich für den Schutz der Infrastruktur ist die Absicherung der Feldkomponenten, des Leitsystems sowie deren Interkommunikation. Die IP-Anbindung von Fernwirkgeräten an das Leitsystem muss gegen Fremdzugriffe geschützt, die Integrität der übertragenden Messwerte und Steuerbefehle sichergestellt, sowie die Authentizität der Kommunikationspartner garantiert werden.

Da Feldkomponenten im EEG-Umfeld typischerweise einen geringeren Objektschutz als Großkraftwerke besitzen, bedarf es zusätzlicher Maßnahmen. Angriffe auf das Leitsystem über die Netzanbindung der Feldkomponente müssen verhindert oder dessen Auswirkungen auf ein beherrschbares Maß begrenzt werden.

Wie hilft Fortinet dabei?

Fortinet bietet mit seinem Portfolio umfassenden Schutz für die Herausforderungen der Energiewende.

Die Absicherung der Steuerungsnetze von Versorgern und Netzbetreibern lässt sich dabei mit Fortinet-Standardlösungen realisieren. Zugunsten von Kosten und Management-Effizienz stellt die FortiGate-Plattform alle zuvor als relevant beschriebenen Schutzmaßnahmen, wie z.B. VPN, IPS, Application Control und DoS Protection, bereit und bietet dafür ein zentrales und hocheffizientes Management. Die Option für Zero-Touch Deployments sowie Schnittstellen zur Integration weiterer und vorhandener Systeme – für die optimale Abbildung von Betriebsprozessen – runden das Portfolio ab.

Zusätzlich erlangt die FortiGate-Plattform über verfügbare „Industrial Signature FortiGuard Subscription Services“ das erforderliche Protokollverständnis für den Einsatz bei Energieversorgern oder Netzbetreibern. Durch diese industriespezifischen OT-Protokolle erhält die FortiGate-Plattform die Möglichkeit, über IEC 60870-5-104 oder IEC 61850 realisierte Unterstationsanbindungen auf Telegrammebene oder auch Leitsystemkopplungen über IEC 60870-6 (TASE.2/ ICCP) zu reglementieren. Darüber hinaus lässt sich das Schutzniveau im Bereich der Telegrammfilterung durch Definition individuell auf die Umgebung angepasster Protokoll-Parameter – wie beispielsweise der verwendeten ADSU-Adressen – erweitern. Damit lässt sich der Ansatz eines positiven Security-Modelles mit expliziter Freischaltung legitimer Telegramme realisieren.

Warum Fortinet

- Anerkannte Lösungen in der Energiewirtschaft
- Deutlich erhöhtes Sicherheitsniveau der im Netz genutzten OT-Verbindungen
- Nahtlos integrierte und leistungsstarke Sicherheit für die gesamte Infrastruktur
- Hohe Bedienfreundlichkeit, einfache Implementierung und langfristige Zukunftssicherheit
- Weiterentwicklung der FortiGate zu einer „Next Generation Prozessnetz Firewall“, die die speziellen Anforderungen von Energieversorgern erfüllt

Fortinet
Feldbergstr. 35
D-60323 Frankfurt am Main

www.fortinet.com/de

December 9, 2021 2:58 PM
1374293-0-1-DE