OT-CYBER.DE

WOCHENBERICHT

OT-/Cyber-Lagebild Strom und Energie

Ausgabe KW 46/2026 · Strom und Energie in DACH

Zielgruppe	Netzbetreiber, Stadtwerke, Erzeuger, Energieversorger
Berichtszeitraum	06.11.2026 bis 13.11.2026
Version	1.0
Datum	13.11.2026
Autor	Maximilian Gilg, OT-Cyber.de
Klassifizierung	TLP:CLEAR, ausschließlich öffentliche Quellen

Dieser Bericht fasst öffentlich zugängliche Meldungen zusammen. Die Einstufung der Relevanz bezieht sich auf Netzbetreiber, Stadtwerke, Erzeuger, Energieversorger in Deutschland, Österreich und der Schweiz.

Management Summary

Im Berichtszeitraum ist ein Cyberangriff auf einen deutschen Versorger bekannt geworden. Die Stadtwerke Achim (Niedersachsen) haben den Vorfall am 08.11.2026 über ihre eigenen Monitoring-Systeme erkannt und sprechen von einem gezielten, kriminellen und professionell durchgeführten Cyberangriff, der zum Ausfall zentraler IT-Systeme geführt hat. Kundenportale und E-Mail sind nicht verfügbar, und die Abschläge für EEG- und KWKG-Anlagen kommen im November nicht pünktlich. Die Versorgung mit Strom, Gas und Fernwärme war laut Stadtwerken zu keiner Zeit betroffen. Für andere Betreiber stellt sich damit die Frage, ob die eigene Trennung zwischen IT und Leittechnik im Ernstfall hält und ob der Notbetrieb ohne IT funktioniert.

Die zweite Linie der Woche ist PHP2Shell (CVE-2026-109618, CVSS 3.1: 9,8). Die Lücke ist jetzt in der Netzleittechnik angekommen: CISA hat am 12.11. das Siemens-Advisory zu Spectrum Power 3, 4, 7 und TG, AMIS TS und Energy Engage neu veröffentlicht. Für mehrere Produkte gibt es noch keinen Fix, für Energy Engage V2.0SP9 ist keiner geplant. Gleichzeitig trifft die Lücke das Fernwartungsportal mbCONNECT24 (Remote Code Execution ohne Anmeldung) und die Weidmüller-Router IE-SR (dort laut Advisory nur ein Denial of Service der Weboberfläche). Dazu führt die CISA seit dem 06.11. eine SonicWall-SSL-VPN-Lücke als aktiv ausgenutzt. Remote Access und Netzleitsysteme haben diese Woche Vorrang.

GESAMTBEWERTUNG

Die Lage ist erhöht: ein bestätigter Cyberangriff auf die IT eines deutschen Versorgers und kritische Lücken in Netzleitsystemen, für die es teilweise noch keinen Patch gibt. Vorrang haben die Abschottung von Spectrum-Power-Umgebungen und die Prüfung aller Fernwartungszugänge (SonicWall, mbCONNECT24, Industrie-Router).

Trends

• PHP2Shell zieht sich durch die ganze Kette: Netzleitsystem (Spectrum Power), Fernwartungsportal (mbCONNECT24) und Stationsrouter (Weidmüller) innerhalb einer Woche.

• In Achim fielen nach dem Angriff Kundenportale, E-Mail und die pünktlichen EEG- und KWKG-Zahlungen aus, die Versorgung lief laut Stadtwerken weiter.

• Fernwartungszugänge (SSL-VPN, Herstellerportale, Mobilfunk-Router) bleiben der wahrscheinlichste Einstieg in die OT.

• Für mehrere Produkte der Netzleittechnik gibt es noch keinen Patch, kompensierende Maßnahmen wie Segmentierung und Monitoring müssen die Zeit bis zum Fix überbrücken.

Lageübersicht

ID	Meldung	Relevanz	Quelle
L-01	Stadtwerke Achim: Cyberangriff auf die zentrale IT, Versorgung laut Unternehmen nicht betroffen	HOCH	Stadtwerke Achim, 08.11.
L-02	PHP2Shell in Siemens-Netzleittechnik: Spectrum Power, AMIS TS und Energy Engage betroffen, teils ohne Fix (ICSA-26-316-01)	KRITISCH	CISA / Siemens ProductCERT (SSA-166980), 12.11.

ID	Meldung	Relevanz	Quelle
L-03	MB connect line mbCONNECT24: Remote Code Execution ohne Anmeldung über gebündeltes PHP (VDE-2026-128, CVSS 9,8)	HOCH	MB connect line, koordiniert von CERT@VDE, 10.11.
L-04	Weidmüller-Security-Router IE-SR: PHP2Shell legt Weboberfläche lahm (VDE-2026-152)	MITTEL	CERT@VDE, 10.11.
L-05	SonicWall SonicOS SSL-VPN: CVE-2026-19868 aktiv ausgenutzt (CISA KEV)	HOCH	CISA, 06.11.
L-06	Welotec egOS: Edge-Gateways vertrauen kompromittierten Zwischenzertifikaten (VDE-2026-138)	NIEDRIG	CERT@VDE, 11.11.

Exponierte OT-Systeme (Shodan)

Exponierte OT-Systeme (Shodan, Stand 13.11.2026):

Gezählt werden aus dem Internet erreichbare Dienste typischer OT-Protokolle. Die Zahlen sind ein Indikator für Angriffsfläche, kein Nachweis einer Verwundbarkeit. Keine Einzelsysteme genannt. Siemens S7 = Port 102 (alle ISO-TSAP-Dienste, nicht nur echte S7-Steuerungen), OPC UA = Standardport 4840.

Region	Gesamt	Top-Protokolle
Deutschland	139840	DNP3: 31446, OMRON FINS: 26419, ProConOS: 15503, Siemens S7: 7574, OPC UA: 4952
Österreich	4663	HMI/VNC: 1007, DNP3: 959, Niagara Fox: 456, Siemens S7: 381, OPC UA: 149

Meldungen im Detail

L-01 Stadtwerke Achim: Cyberangriff auf die zentrale IT, Versorgung laut Unternehmen nicht betroffen

HOCH Stadtwerke Achim, 08.11.

Was ist neu: Die Stadtwerke Achim haben den Angriff am 08.11.2026 über ihre eigenen Monitoring-Systeme erkannt. Sie sprechen von einem gezielten, kriminellen und professionell durchgeführten Cyberangriff, der zum Ausfall zentraler IT-Systeme geführt hat. Alle IT-Systeme wurden isoliert, das BSI und die Landesdatenschutzbeauftragte sind informiert. Kundenportale und E-Mail sind nicht verfügbar, die Abschläge für EEG- und KWKG-Anlagen kommen im November nicht pünktlich.

Bedeutung: Laut Stadtwerken war die Versorgung mit Strom, Gas und Fernwärme zu keiner Zeit betroffen. Wie die Leittechnik in Achim angebunden ist, ist nicht öffentlich. Unsere Einschätzung allgemein: Ob ein Netz nach einem Angriff auf die Büro-IT weiterläuft, hängt davon ab, wie sauber IT und Leittechnik getrennt sind.

Empfehlung: Nachweisen, dass es keine dauerhafte Verbindung aus der Büro-IT in die Leittechnik gibt (gemeinsames Active Directory, Jump Host, Datei-Shares), und den Notbetrieb bei isolierter Büro-IT üben, inklusive Abrechnung, Einspeisevergütung und BSI-Meldung (CC2, CC1).

Quelle: https://www.stadtwerke-achim.de/de/Unternehmen/Aktuelles/Wichtige-News/ ✓ geprüft

L-02 PHP2Shell in Siemens-Netzleittechnik: Spectrum Power, AMIS TS und Energy Engage betroffen, teils ohne Fix (ICSA-26-316-01)

KRITISCH CISA / Siemens ProductCERT (SSA-166980), 12.11.

Was ist neu: CISA hat das Siemens-Advisory zu CVE-2026-109618 (CVSS 9,8) und CVE-2026-109619 (CVSS 8,1) im Sektor Energy neu veröffentlicht. Betroffen sind Spectrum Power 3, 4, 7 und TG, AMIS TS, Energy Engage und blueplanet-Wechselrichter. Für Energy Engage V2.0SP9 ist kein Fix geplant, für AMIS TS, blueplanet 360 und Spectrum Power 4 gibt es noch keinen.

Bedeutung: Spectrum Power ist in vielen Netzleitstellen im Einsatz. Die Lücken sitzen in der PHP-Laufzeit, die zum Beispiel im Infrastruktur-Monitoring (IHM/NagiosXI) mitläuft, und erlauben Code-Ausführung ohne Anmeldung. Wer aus dem Leitsystem-Netz eine dieser Komponenten erreicht, hat damit einen Weg in den Kern der Leittechnik.

Empfehlung: Beim Systemlieferanten klären, welche Spectrum-Power- und Monitoring-Komponenten PHP nutzen, und die verfügbaren Red-Hat- bzw. PHP-Updates einplanen (CC5). Bis dahin den Zugriff auf die Weboberflächen auf feste Admin-Hosts begrenzen und den Verkehr dorthin überwachen (CC2, CC3).

Quelle: https://www.cisa.gov/news-events/ics-advisories/icsa-26-316-01 ✓ geprüft

L-03 MB connect line mbCONNECT24: Remote Code Execution ohne Anmeldung über gebündeltes PHP (VDE-2026-128, CVSS 9,8)

HOCH MB connect line, koordiniert von CERT@VDE, 10.11.

Was ist neu: mbCONNECT24 und mymbCONNECT24 ab Version 2.0.0 und vor 2.21.6 enthalten ein PHP mit CVE-2026-109618 (CVSS 3.1: 9,8) und CVE-2026-109619 (CVSS 3.1: 8,1). Laut Advisory können beide Lücken zu Remote Code Execution ohne Anmeldung führen. Behoben ist das in Version 2.21.6. Eine Ausnutzung meldet das Advisory nicht.

Bedeutung: Über solche Portale warten Anlagenbauer BHKW, Wärmeerzeuger, Pumpen und Nebenanlagen in Umspannwerken. Ein übernommenes Portal öffnet auf einen Schlag den Weg zu allen angebundenen Anlagen mehrerer Betreiber.

Empfehlung: Eine Liste aller Dienstleister mit eigenem Fernzugang führen und schriftlich den Patch-Stand des Portals abfragen. Zugänge nur bei Bedarf freischalten und Sitzungen protokollieren (CC4).

Quelle: https://certvde.com/en/advisories/VDE-2026-128/ ✓ geprüft

L-04 Weidmüller-Security-Router IE-SR: PHP2Shell legt Weboberfläche lahm (VDE-2026-152)

MITTEL CERT@VDE, 10.11.

Was ist neu: In den Security-Routern IE-SR-4TX und IE-SR-4GT vor Firmware 2.3.4 steckt CVE-2026-109618. Laut CERT@VDE kann ein Angreifer damit die Weboberfläche zeitweise lahmlegen, Code ausführen kann er nicht. Behoben ist das in Firmware 2.3.4.

Bedeutung: Solche Hutschienen-Router sitzen oft als Zugang in Ortsnetz- und Umspannstationen. Routing und Firewall laufen laut Advisory weiter, aber ohne Weboberfläche ist die Fernverwaltung im Ernstfall eingeschränkt.

Empfehlung: Router im Asset-Inventar suchen, Firmware 2.3.4 einplanen und die Weboberfläche nur aus dem Management-Netz erreichbar machen (CC5, CC4).

Quelle: https://certvde.com/en/advisories/VDE-2026-152/ ✓ geprüft

L-05 SonicWall SonicOS SSL-VPN: CVE-2026-19868 aktiv ausgenutzt (CISA KEV)

HOCH CISA, 06.11.

Was ist neu: Die CISA hat am 06.11. CVE-2026-19868 in SonicOS SSLVPN („Use of Single-factor Authentication“) in den KEV-Katalog aufgenommen, weil es Belege für aktive Ausnutzung gibt. Betroffene Versionen nennt die Meldung nicht.

Bedeutung: SonicWall-Firewalls sind bei kleineren Stadtwerken und Netzbetreibern oft das VPN-Gateway für Fernwartung und Bereitschaft. Ein übernommener VPN-Zugang ist ein direkter Initial Access ins Netz und je nach Segmentierung bis in die Leittechnik.

Empfehlung: Herstellerhinweis zu CVE-2026-19868 lesen und patchen, phishing-resistente MFA am SSL-VPN erzwingen und die VPN-Logs der letzten Wochen auf Anmeldungen zu ungewöhnlichen Zeiten oder aus fremden Ländern prüfen (CC4).

Quelle: https://www.cisa.gov/news-events/alerts/2026/11/06/cisa-adds-one-known-exploited-vulnerability-catalog ✓ geprüft

L-06 Welotec egOS: Edge-Gateways vertrauen kompromittierten Zwischenzertifikaten (VDE-2026-138)

NIEDRIG CERT@VDE, 11.11.

Was ist neu: Der Trust Store von egOS übernimmt die Mozilla-NSS-Wurzeln und enthält eMudhra-emSign-Zertifikate, deren Schlüssel für acht Zwischen-CAs kompromittiert sind. Betroffen sind egOS-Versionen vor 1.11.2 (CVE-2026-113470, CVSS 5,4).

Bedeutung: Wer einen dieser Schlüssel besitzt und den Verkehr mitlesen kann, kann ausgehende TLS-Verbindungen der Gateways übernehmen. Das betrifft Gateways, die Messwerte aus PV-, Wind- oder Netzanlagen per TLS weitergeben.

Empfehlung: egOS im nächsten Wartungsfenster auf 1.11.2 heben und prüfen, ob die Gateways nur mit fest hinterlegten Zielen sprechen (CC5).

Quelle: https://certvde.com/en/advisories/VDE-2026-138/ ✓ geprüft

Empfehlungen

Nr.	Maßnahme	Bezug	Priorität	Zeitraum
M-01	Notbetrieb bei isolierter Office-IT üben, inklusive Abrechnung, Einspeisevergütung und BSI-Meldung [CC1 ICS Incident Response]	L-01	HOCH	0 bis 3 Monate
M-02	Spectrum-Power-Umgebung abschotten und verfügbare PHP-Patches einspielen; für Produkte ohne Fix kompensierende Maßnahmen dokumentieren (CC5, CC2)	L-02	HOCH	sofort
M-03	Router und Edge-Gateways in Stationen (Weidmüller, Welotec) in den Patch-Zyklus aufnehmen (CC5)	L-04	MITTEL	0 bis 3 Monate
M-04	SonicWall-SSL-VPN patchen, phishing-resistente MFA erzwingen und VPN-Logs seit Anfang November auswerten [CC4 Secure Remote Access]	L-05	HOCH	sofort

Fragen für das nächste Jour fixe

1. Welche Komponenten unseres Netzleitsystems nutzen PHP, und was sagt der Lieferant zu SSA-166980?

2. Könnte unsere Leitstelle weiterarbeiten, wenn wir die gesamte Office-IT wie in Achim isolieren müssten?

3. Welche Dienstleister haben einen eigenen Fernzugang, und über welches Portal bzw. VPN läuft er?

4. Haben wir SonicWall-SSL-VPN im Einsatz, und wurden die Logs nach dem 06.11. geprüft?

5. Wie zahlen wir EEG- und KWKG-Einspeiser aus, wenn das Abrechnungssystem zwei Wochen ausfällt?

Maßnahmen dieser Woche

1. Spectrum-Power-, AMIS-TS- und Energy-Engage-Systeme erfassen, Lieferant zu PHP-Patches befragen und Zugriff auf feste Admin-Hosts begrenzen.

2. SonicOS patchen und alle SSL-VPN-Konten auf phishing-resistente MFA umstellen.

3. Dienstleister mit mbCONNECT24 oder anderen Portalen schriftlich nach Version 2.21.6 bzw. dem Patch-Stand fragen.

4. Weidmüller-, Welotec- und andere Stationsrouter im Asset-Inventar suchen und Firmware-Updates einplanen.

5. Die Trennung zwischen Office-IT und Leittechnik gegen die Firewall-Regeln abgleichen und undokumentierte Verbindungen schließen.

6. Ein kurzes Tabletop zum Szenario „IT isoliert, Leitstelle läuft“ inklusive BSI-Meldung durchführen.

HINWEIS ZUR QUELLENLAGE

Die Meldungen stützen sich auf Primärquellen (Stadtwerke Achim, Seite „Wichtige News“, Stand 13.11.2026, https://www.stadtwerke-achim.de/de/Unternehmen/Aktuelles/Wichtige-News/; CISA; Siemens ProductCERT; CERT@VDE). Den Verdacht auf Ransomware in Achim nennt nur buten un binnen (https://www.butenunbinnen.de/nachrichten/cyberangriff-achim-stadtwerke-100.html), die Stadtwerke äußern sich dazu wegen der laufenden Ermittlungen nicht; einen dort erwähnten Angriff auf einen Solarpark in Thüringen haben wir nicht gefunden (nur ein physischer Einbruch in Altenburg, https://altenburg.tv/polizeinachrichten/zugangstor-zu-solarpark-gewaltsam-geoeffnet/). Nicht aufgenommen: der Leak-Site-Eintrag zu den Stadtwerken Waldbröl (Incransom, 12.11., nicht bestätigt, https://www.ransomware.live/id/U3RhZHR3ZXJrZSBXYWxkYnLDtmwgR21iSEBpbmNyYW5zb20), die nur in der Presse belegte französische Zuordnung der Kühlanlagen-Angriffe an die IRGC sowie OpenSSH „SSHole“ (Embedded-Linux, ohne bekannte Ausnutzung); zu NCSC Schweiz und E-Control haben wir in KW 46 keine Energiewarnung gefunden. Alle Quellenlinks wurden am 13.11.2026 automatisch aufgerufen und inhaltlich geprüft. Achim und SonicWall haben wir am 13.11. an den Primärquellen nachgeprüft und aufgenommen. Siemens Gridscale X bleibt draußen, weil der Beleg fehlt.