OT-CYBER.DE

WOCHENBERICHT

OT-/Cyber-Lagebild Kommunale Versorger und KRITIS

Ausgabe KW 46/2026 · Kommunale Versorger und KRITIS in DACH

Zielgruppe	Stadtwerke, Wasser- und Abwasserbetriebe, KRITIS-Betreiber
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 Stadtwerke, Wasser- und Abwasserbetriebe, KRITIS-Betreiber in Deutschland, Österreich und der Schweiz.

Management Summary

Im Berichtszeitraum ist ein Cyberangriff auf einen kommunalen Versorger in Deutschland bekannt geworden. Die Stadtwerke Achim in Niedersachsen haben den Angriff am 08.11.2026 erkannt, seitdem sind zentrale IT-Systeme, Kundenportale und E-Mail nicht verfügbar. Laut buten un binnen geht die Zentralstelle Cybercrime Niedersachsen dem Verdacht eines Ransomware-Angriffs nach, die Stadtwerke selbst äußern sich dazu wegen der laufenden Ermittlungen nicht. Strom, Gas und Fernwärme waren laut Unternehmen 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 an der Trennung zwischen IT und OT.

Bei den Schwachstellen ging es diese Woche vor allem um Fernwartung. Das Fernwartungsportal mbCONNECT24 hat zwei PHP2Shell-Lücken mit Remote Code Execution ohne Anmeldung (CVSS 3.1: 9,8 und 8,1), im Helmholz-Fernwartungsserver myREX24V2 stecken 12 Schwachstellen, SonicWall-SSL-VPN wird laut CISA aktiv ausgenutzt, und OpenSSH lässt sich auf Linux-Systemen mit musl libc ohne PAM mit überlangen Passwörtern umgehen. Für WinCC V7.5 bis V8.1 gibt es eine Lücke ohne Patch. Frankreich macht für die Kühlanlagen-Angriffe vom Oktober auf französische Geschäfte eine IRGC-nahe Einheit verantwortlich, die spätere Welle im November ist nicht zugeordnet.

GESAMTBEWERTUNG

Die Lage ist erhöht, weil es einen bestätigten Cyberangriff auf die IT eines deutschen Stadtwerks gibt und mehrere kritische Lücken genau die Fernzugänge in die OT betreffen. Vorrang haben die Fernwartungsportale (mbCONNECT24, myREX24) und VPN-Gateways (SonicWall) sowie der Check, ob die Trennung von IT und OT im eigenen Haus hält.

Trends

• Die Fernwartung ist diese Woche der größte Angriffspunkt: Fernwartungsportale, Fernwartungsserver und VPN-Gateways tauchen gleich mehrfach mit kritischen Lücken auf.

• PHP2Shell zieht sich durch die Industrie-Produkte, CERT@VDE veröffentlicht laufend neue betroffene Geräte, mit Auswirkungen von Denial of Service bis Remote Code Execution.

• Angriffe auf die Büro-IT legen bei Stadtwerken Portale und Abrechnung lahm. Ob das Netz weiterläuft, hängt nach unserer Einschätzung an der Trennung zur Leittechnik.

• Mit der französischen Zuordnung der Oktober-Angriffe ist bei fernwartbarer Kältetechnik ein staatlicher Akteur benannt. Diese Technik läuft in vielen Betrieben außerhalb von IT- und OT-Security.

• Lücken in Embedded-Linux wie SSHole kommen bei Edge-Geräten erst mit großer Verzögerung über die Firmware der Hersteller an.

Lageübersicht

ID	Meldung	Relevanz	Quelle
L-01	MB connect line mbCONNECT24: Remote Code Execution ohne Anmeldung über gebündeltes PHP (VDE-2026-128, CVSS 9,8)	KRITISCH	MB connect line, koordiniert von CERT@VDE, 10.11.

ID	Meldung	Relevanz	Quelle
L-02	Stadtwerke Achim: Cyberangriff auf die zentrale IT, Versorgung laut Unternehmen nicht betroffen	HOCH	Stadtwerke Achim / buten un binnen, 08.11.
L-03	SonicWall SonicOS SSLVPN: CVE-2026-19868 wird aktiv ausgenutzt (CISA KEV)	HOCH	CISA, 06.11.
L-04	Helmholz myREX24V2: 12 Schwachstellen im Fernwartungsserver, bis CVSS 4.0 8,7 (VDE-2026-141)	HOCH	CERT@VDE, 10.11.
L-05	OpenSSH „SSHole“: Login ohne gültiges Passwort auf Linux mit musl libc ohne PAM (behoben in OpenSSH 10.6p2)	HOCH	OpenSSH (oss-security) / SecurityWeek, 06.11.
L-06	Siemens SIMATIC WinCC Graphics Designer: Code-Ausführung beim Öffnen einer Datei, kein Fix für V7.5 bis V8.1 (SSA-979641)	MITTEL	Siemens ProductCERT, 10.11.
L-07	Kühlanlagen-Angriffe: Frankreich macht IRGC-nahe Einheit „Shahid Kaveh“ verantwortlich	MITTEL	BleepingComputer, 09.11.

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

KRITISCH 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: Ein Fernwartungsportal hat Verbindungen zu vielen Anlagen gleichzeitig. Wer das Portal übernimmt, kommt im schlimmsten Fall in alle angebundenen Steuerungen, auch zu Pumpwerken, Hochbehältern und Kläranlagen. Nach unserer Erfahrung betreiben viele Stadtwerke das Portal nicht selbst, sondern nutzen das ihres Anlagenbauers. Dann sehen sie die Lücke gar nicht.

Empfehlung: Im Asset-Inventar und in den Wartungsverträgen nachsehen, welche Dienstleister mbCONNECT24 oder mymbCONNECT24 nutzen, und schriftlich bestätigen lassen, dass Version 2.21.6 läuft. Bis dahin die Fernwartungsverbindung nur bei Bedarf freischalten (CC4 Secure Remote Access).

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

L-02 Stadtwerke Achim: Cyberangriff auf die zentrale IT, Versorgung laut Unternehmen nicht betroffen

HOCH Stadtwerke Achim / buten un binnen, 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. Laut buten un binnen (12.11.) geht die Zentralstelle Cybercrime Niedersachsen dem Verdacht eines Ransomware-Angriffs nach. Die Stadtwerke äußern sich dazu wegen der laufenden Ermittlungen nicht.

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-03 SonicWall SonicOS SSLVPN: CVE-2026-19868 wird aktiv ausgenutzt (CISA KEV)

HOCH CISA, 06.11.

Was ist neu: Die CISA hat CVE-2026-19868 in SonicOS SSLVPN („Use of Single-factor Authentication“) am 06.11. in ihren KEV-Katalog aufgenommen. Grundlage sind Belege für aktive Ausnutzung.

Bedeutung: Wo SonicWall-Firewalls das VPN-Gateway für Fernwartung oder Bereitschaftsdienst sind, ist ein kompromittierter Zugang ein direkter Initial Access ins Netz und je nach Segmentierung bis in die OT. Gerade kleine Stadtwerke und Zweckverbände haben oft nur dieses eine Gateway.

Empfehlung: SonicOS nach Hersteller-Advisory aktualisieren, für alle SSL-VPN-Konten phishing-resistente MFA erzwingen und die VPN-Logs der letzten Wochen auf Anmeldungen von unbekannten IPs oder zu ungewöhnlichen Zeiten prüfen (CC4 Secure Remote Access, CC5 Risk-Based Vulnerability Management).

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

L-04 Helmholz myREX24V2: 12 Schwachstellen im Fernwartungsserver, bis CVSS 4.0 8,7 (VDE-2026-141)

HOCH CERT@VDE, 10.11.

Was ist neu: In myREX24V2 und myREX24V2.virtual mit Firmware unter 2.21.0 stecken 12 Schwachstellen (CVE-2026-60035 bis CVE-2026-60046). Die höchste Bewertung nach CVSS 4.0 ist 8,7. Das Cross-Site Scripting CVE-2026-60043 bewertet das Advisory nach CVSS 3.1 mit 9,3, im CVE-Eintrag steht dafür CVSS 4.0 6,4. Dazu kommen OS Command Injection (nur mit hohen Rechten), CSRF, ein Standardpasswort für Backups und eine schwache Passwort-Wiederherstellung.

Bedeutung: myREX24 ist ein zentraler Fernwartungsserver, über den Wartungsfirmen auf Steuerungen in Pumpwerken und Kläranlagen zugreifen. Laut Advisory können die Lücken zum vollständigen Verlust von Vertraulichkeit, Integrität und Verfügbarkeit führen. Ob sie schon ausgenutzt werden, sagt das Advisory nicht.

Empfehlung: Eigene und von Dienstleistern betriebene myREX24-Instanzen auf 2.21.0 oder neuer bringen und die Weboberfläche nur aus bekannten Netzen erreichbar machen. Gleich mit klären, wer im Notfall den Fernwartungsserver abschaltet (CC4 Secure Remote Access).

Quelle: https://certvde.com/en/advisories/VDE-2026-141/ ✓ geprüft

L-05 OpenSSH „SSHole“: Login ohne gültiges Passwort auf Linux mit musl libc ohne PAM (behoben in OpenSSH 10.6p2)

HOCH OpenSSH (oss-security) / SecurityWeek, 06.11.

Was ist neu: Die Lücke betrifft sshd auf Linux-Systemen mit musl libc und abgeschaltetem PAM, laut SecurityWeek unter anderem Alpine, OpenWrt, Buildroot und Yocto. Mit einem Passwort von 257 bis 1.024 Zeichen ist unter bestimmten Bedingungen eine Anmeldung möglich. Behoben ist das in OpenSSH 10.6p2, Alpine hat am 05.11. zum Patchen aufgerufen. Eine Ausnutzung ist laut Detectify noch nicht bekannt, die Details sind aber öffentlich.

Bedeutung: Genau auf diesen Linux-Varianten laufen viele Industrie-Router, Fernwirk-Gateways und Edge-Geräte in Wasserwerken und Ortsnetzstationen. Für solche Geräte kommt der Fix nicht über die Distribution, sondern muss von jedem Hersteller einzeln in die Firmware eingebaut werden. Nach unserer Erfahrung dauert das Wochen.

Empfehlung: Im Asset-Inventar alle Geräte mit erreichbarem SSH markieren, bei den Herstellern nach dem Firmware-Stand mit OpenSSH 10.6p2 fragen und SSH bis dahin nur aus dem Verwaltungsnetz zulassen (CC5 Risk-Based Vulnerability Management).

Quelle: https://www.securityweek.com/openssh-rushes-patches-for-sshole-authentication-bypass/ ✓ geprüft

L-06 Siemens SIMATIC WinCC Graphics Designer: Code-Ausführung beim Öffnen einer Datei, kein Fix für V7.5 bis V8.1 (SSA-979641)

MITTEL Siemens ProductCERT, 10.11.

Was ist neu: Der Graphics Designer in SIMATIC WinCC V7.5, V8.0 und V8.1 (alle Versionen) kann beim Öffnen einer präparierten Datei Code ausführen (CVE-2026-59082, CVSS 3.1 7,8). Siemens bereitet Fixes vor, bis dahin gibt es nur Mitigations.

Bedeutung: WinCC ist in Wasser- und Abwasserbetrieben und bei Fernwärme weit verbreitet. Der Angriff braucht eine präparierte Datei, die jemand öffnet, zum Beispiel ein Projektstand von einem Integrator, ein Mail-Anhang oder ein USB-Stick. Engineering-Stationen mit Mail und Internet sind deshalb besonders gefährdet.

Empfehlung: Projekt- und Grafikdateien nur aus festen, bekannten Quellen übernehmen (Übergabe über eine Prüfstation statt Mail oder USB) und die Engineering-Stationen ohne Mail- und Internetzugang betreiben, bis der Fix da ist (CC2 Defensible Architecture).

Quelle: https://cert-portal.siemens.com/productcert/html/ssa-979641.html ✓ geprüft

L-07 Kühlanlagen-Angriffe: Frankreich macht IRGC-nahe Einheit „Shahid Kaveh“ verantwortlich

MITTEL BleepingComputer, 09.11.

Was ist neu: Laut BleepingComputer schreibt Frankreich die Angriffe vom Oktober auf Kühlsysteme in rund 700 angegriffenen Supermärkten und anderen Geschäften der Einheit Shahid Kaveh zu, die den iranischen Revolutionsgarden (IRGC) nahesteht. Die Angreifer haben laut Bericht Danfoss-Kühlsteuerungen kompromittiert und die Abtau-Einstellungen aus der Ferne auf hohe Temperaturen gestellt. Mindestens 15 Brände werden den Angriffen zugeordnet. Die spätere Welle im November mit über 115 Geschäften in sechs europäischen Ländern ist nicht zugeordnet.

Bedeutung: Damit sind die Oktober-Angriffe in Frankreich einem staatlichen Akteur zugeordnet. Stadtwerke betreiben selbst Kälte- und Klimaanlagen in Rechenzentren, Bädern, Leitwarten und Kläranlagen, oft mit Fernzugang des Kälteanlagenbauers, den in der IT niemand auf dem Schirm hat. Die Erklärung des Ministeriums selbst haben wir nicht eingesehen, der Beleg ist der Pressebericht.

Empfehlung: Alle Kälte- und Gebäudeleittechnik-Controller mit Fernzugang erfassen, Zugänge aus dem Internet schließen und Hersteller-Fernwartung über den zentralen, protokollierten Fernwartungsweg führen (CC4 Secure Remote Access, CC3 ICS Network Visibility & Monitoring).

Quelle: https://www.bleepingcomputer.com/news/security/france-blames-iranian-hackers-for-supermarket-attacks-that-sparked-fires/ ✓ geprüft

Empfehlungen

Nr.	Maßnahme	Bezug	Priorität	Zeitraum
M-01	Alle Fernwartungsportale und -server (mbCONNECT24, myREX24) eigener und fremder Betreiber auf gepatchte Versionen bringen und Fernwartung nur bei Bedarf freischalten [CC4 Secure Remote Access]	L-01	HOCH	sofort
M-02	SonicWall-SSL-VPN patchen, phishing-resistente MFA erzwingen, VPN-Logs auswerten [CC4 Secure Remote Access]	L-03	HOCH	sofort
M-03	Trennung zwischen Büro-IT und Leittechnik prüfen und den Incident-Response-Plan für einen Ausfall der Büro-IT bei laufendem Netz üben [CC1 ICS Incident Response]	L-02	HOCH	0 bis 3 Monate
M-04	Edge-Geräte mit Embedded-Linux und SSH im Asset-Inventar erfassen und Firmware-Updates nach Risiko priorisieren [CC5 Risk-Based Vulnerability Management]	L-05	MITTEL	0 bis 3 Monate
M-05	Kälte- und Gebäudeleittechnik mit Fernzugang ins OT-Monitoring aufnehmen und über den zentralen Fernwartungsweg führen [CC3 ICS Network Visibility & Monitoring]	L-07	MITTEL	3 bis 6 Monate

Fragen für das nächste Jour fixe

1. Welche unserer Dienstleister nutzen mbCONNECT24, mymbCONNECT24 oder myREX24, und welche Version läuft dort heute?

2. Könnten wir wie die Stadtwerke Achim Strom, Gas, Wasser und Wärme weiterbetreiben, wenn morgen die komplette Büro-IT ausfällt, und wer entscheidet das?

3. Welche Kälte-, Klima- und Gebäudeleittechnik hat einen Fernzugang des Herstellers, der nicht über unseren zentralen Fernwartungsweg läuft?

4. Ist auf unserem VPN-Gateway für alle Konten phishing-resistente MFA aktiv, und wer wertet die VPN-Logs aus?

5. Wie bekommen Projektdateien von Integratoren auf unsere WinCC-Engineering-Stationen, und wird dabei etwas geprüft?

Maßnahmen dieser Woche

1. Dienstleister mit mbCONNECT24/mymbCONNECT24 anschreiben und Version 2.21.6 schriftlich bestätigen lassen, eigene myREX24V2-Instanzen auf 2.21.0 oder neuer bringen.

2. SonicWall-SSL-VPN nach Hersteller-Advisory patchen, MFA für alle Konten erzwingen und die Logins der letzten Wochen auf Auffälligkeiten prüfen.

3. Schriftlich nachweisen, welche Verbindungen es zwischen Büro-IT und Leittechnik gibt (AD-Vertrauensstellungen, Jump Hosts, Shares), und unnötige kappen.

4. Im Asset-Inventar alle Router, Gateways und Edge-Geräte mit erreichbarem SSH markieren und bei den Herstellern den Patch-Stand für OpenSSH 10.6p2 erfragen.

5. Für WinCC-Engineering-Stationen den Mail- und Internetzugang prüfen und eine feste Übergabe für Projektdateien festlegen.

6. Fernzugänge der Kälte- und Gebäudeleittechnik erfassen und aus dem Internet erreichbare Controller abschalten oder hinter den zentralen Fernwartungsweg legen.

HINWEIS ZUR QUELLENLAGE

Die Advisories (CERT@VDE, Siemens, CISA KEV) sind Primärquellen; zum Fall Achim haben wir die Primärquelle der Stadtwerke geprüft (https://www.stadtwerke-achim.de/de/Unternehmen/Aktuelles/Wichtige-News/, Stand 13.11.2026), den Ransomware-Verdacht nennt nur die Presse (buten un binnen, https://www.butenunbinnen.de/nachrichten/cyberangriff-achim-stadtwerke-100.html; Weser-Kurier vom 11.11., https://www.weser-kurier.de/landkreis-verden/stadt-achim/cyberangriff-auf-achimer-stadtwerke-it-systeme-lahmgelegt-doc88feidafgmdhl0xoarw), und die französische Zuschreibung kennen wir nur aus der Presse. Nicht aufgenommen, weil unbestätigt oder außerhalb des Sektors: Stadtwerke Waldbröl steht seit 12.11. auf der Leak-Seite von Incransom (geschätzter Angriff 17.10.), eine Bestätigung des Unternehmens haben wir nicht gefunden (https://www.ransomware.live/id/U3RhZHR3ZXJrZSBXYWxkYnLDtmwgR21iSEBpbmNyYW5zb20); BBT SE (Brenner-Basistunnel) hat einen Datenzugriff vom 17.10. bestätigt, die Zuordnung zu Everest ist unbestätigt. Zu Versorgern in Österreich und der Schweiz haben wir im Zeitraum keine Vorfälle gefunden, ebenso keine neue CISA-ICS-Advisory nach ICSA-26-307-01 (03.11.) und keine neuen bestätigten Vorfälle der US-Wasser-Kampagne; die PHP2Shell-Meldungen zu Weidmüller und ads-tec (nur Denial of Service) sowie Welotec egOS (VDE-2026-138) stammen aus den Tagesbriefings und wurden hier nicht erneut geprüft. Alle Quellenlinks wurden am 13.11.2026 automatisch aufgerufen und inhaltlich geprüft.