VORFALL-LAGEBILD

Cyberangriff auf Stadtwerke Achim: zentrale IT-Systeme lahmgelegt

Stand 12.11.2026 18:18 · Sendung: – · · Belegstärke: bestätigt · berichtet · vermutet · Prozent: 100 = bestätigt, 0 = sicher falsch

Einordnung

1. Nach allem, was bekannt ist, hat die Trennung zwischen Büro-IT und Versorgung in Achim gehalten, Strom, Gas und Fernwärme laufen.

2. Achim reiht sich in eine Serie von Angriffen auf Stadtwerke ein, die Täter suchen offene Türen, nicht bestimmte Städte.

3. Kleine Versorger müssen nicht alles machen, aber fünf Dinge richtig: geübter Notfallplan, saubere Netztrennung, Überwachung, sichere Fernzugänge und Patches nach Risiko.

Was sich seit der Erstmeldung geändert hat

Frühere Aussage	vorher	jetzt	Status
Die Monitoring-Systeme der Stadtwerke Achim haben am Sonntag, 8. November, einen gezielten Cyberangriff erkannt; laut Unternehmen fand er „Ende vergangener Woche“ statt.	100 %	100 %	bestätigt
Die Stadtwerke haben alle Außenverbindungen getrennt und sämtliche IT-Systeme isoliert. Ein Krisenstab mit externen, zertifizierten Spezialisten für Incident Response und IT-Forensik wurde gebildet.	100 %	100 %	bestätigt
Wegen der laufenden IT-forensischen Untersuchung äußert sich das Unternehmen nicht zu Tätern und Forderungen.	100 %	100 %	präzisiert
Die Website der Stadtwerke verweist auf „wichtige Informationen zum aktuellen IT-Vorfall“ und meldet: „Derzeit sind unsere Kundenportale nicht erreichbar“.	100 %	95 %	bestätigt
Es handelt sich um einen finanziell motivierten Angriff mit Erpressungsabsicht (Ransomware oder Datendiebstahl mit Drohung, die Daten zu veröffentlichen).	70 %	72 %	offen
Achim war kein gezielt ausgesuchtes politisches Ziel, sondern ein Opfer, weil der Zugang möglich war.	55 %	58 %	offen
Zentrale IT-Systeme sind ausgefallen, die Kundenportale (Kundenkonto, Zählerstand) sind nicht verfügbar, und die E-Mail-Kommunikation ist gestört. Telefonisch sind die Stadtwerke erreichbar, Anrufe werden dokumentiert und zurückgerufen.	100 %	100 %	bestätigt
Strom, Gas, Fernwärme und Warmwasser sind laut Stadtwerken nicht betroffen, die Versorgung ist gewährleistet.	100 %	100 %	bestätigt

Frühere Aussage	vorher	jetzt	Status
Laut Unternehmen gibt es derzeit „keine Anhaltspunkte“, dass Systeme von Kunden und Partnern betroffen sind. Kunden sollen bei unerwarteter Kontaktaufnahme keine sensiblen Informationen herausgeben.	100 %	95 %	bestätigt
Die Stadtwerke Achim versorgen Kunden in Achim, Oyten, Langwedel und Ottersberg.	100 %	80 %	präzisiert
Kunden müssen sich auf Verzögerungen bei Abrechnung, Zählerstandsmeldungen und Vertragsänderungen einstellen.	75 %	75 %	offen
Nach dem Angriff folgen Phishing-Versuche, die sich auf den Vorfall berufen.	50 %	52 %	offen
Daten wurden abgezogen.	40 %	28 %	offen
Die Stadtwerke Achim nennen keinen Zeitpunkt für die Wiederherstellung.	100 %	100 %	bestätigt
Vergleich Detmold: Angriff im November 2025, laut ZfK sind seit Anfang 2026 alle Systeme wieder erreichbar.	100 %	100 %	bestätigt
Vergleich Neumünster: Telefon nach rund einer Woche wieder verfügbar, Systeme etwa vier Wochen später noch im Wiederaufbau.	100 %	60 %	offen
Telefon und einzelne Dienste sind innerhalb von ein bis zwei Wochen wieder da, der vollständige Normalbetrieb der IT dauert mehrere Wochen bis etwa zwei Monate.	65 %	63 %	präzisiert
Die Kundenportale bleiben länger offline als interne Systeme.	55 %	55 %	offen
Laut Stadtwerken sind Strom, Gas, Fernwärme und Warmwasser nicht betroffen, die Energieversorgung ist nicht Teil des IT-Vorfalls.	100 %	100 %	bestätigt
Physische Anlagen wie Trafostationen, Gasdruckregelanlagen oder Heizwerke sind nicht beschädigt.	85 %	85 %	offen
Der Betrieb läuft mit mehr Handarbeit, etwa bei Störungsannahme, Einsatzplanung oder Messwertabrechnung.	45 %	45 %	offen
Der Verband kommunaler Unternehmen (VKU) hatte im Juli 2025 rund 1.600 Mitgliedsunternehmen (Energie, Wasser, Abfall, Telekommunikation).	100 %	100 %	bestätigt
Seit Inkrafttreten des NIS-2-Umsetzungsgesetzes am 6. Dezember 2025 rechnet das BSI mit rund 29.500 beaufsichtigten Einrichtungen in Deutschland.	100 %	90 %	bestätigt
Allein in den letzten zwölf Monaten wurden unter anderem die Stadtwerke Detmold (November 2025), die Vereinigten Stadtwerke (November 2025) und die Stadtwerke Landsberg (September 2026) angegriffen.	100 %	100 %	bestätigt

Frühere Aussage	vorher	jetzt	Status
Die Zahl der öffentlich bekannten Angrif… (Eingabe abgeschnitten, Aussage unvollständig)	unbekannt %	45 %	offen

Neu seit dem letzten Stand

• buten un binnen (12.11.): Zentralstelle Cybercrime Niedersachsen ermittelt, Ransomware-Verdacht; Stadtwerke sprechen von „gezieltem, kriminellem und professionellem Angriff“.

• Betreiber-Meldung: keine Anhaltspunkte für Abfluss personenbezogener Daten, Experten halten Veröffentlichung für unwahrscheinlich, Darknet-Monitoring läuft; E-Mail derzeit nicht verfügbar; Meldung nach Art. 33 DSGVO.

• Bis 12.11. kein Leak-Site-Eintrag zu Achim gefunden.

• Korrektur: Heinsberg (Januar 2026) betraf die Stadtverwaltung, nicht Stadtwerke.

• Korrektur: Neumünster-Vergleich stammt aus 2023, nicht aus den letzten zwölf Monaten.

Wissensstand



Wissen 43 % Wahrscheinlich 24 % Nicht bekannt 33 %

Die Kernfakten sind durch die eigene Meldung der Stadtwerke (Stand 11.11.2026) und zwei regionale Medien belegt; zu Ursache, Täter, Verschlüsselung und Dauer der Wiederherstellung gibt es keine belastbaren Angaben.

1. Was ist passiert, und warum?

WISSEN

• Die eigenen Monitoring-Systeme haben den Angriff am 08.11.2026 erkannt. (100 %) [https://www.stadtwerke-achim.de/de/Unternehmen/Aktuelles/Wichtige-News/Wichtige-News_219387.html]

• Laut Unternehmen fand der Angriff „Ende vergangener Woche“ statt; danach fielen zentrale IT-Systeme aus. (100 %) [https://www.weser-kurier.de/landkreis-verden/stadt-achim/cyberangriff-auf-achimer-stadtwerke-it-systeme-lahmgelegt-doc88feidafgmdhl0xoarw]

• Alle Außenverbindungen sind getrennt, die IT-Systeme isoliert. Ein interner Krisenstab arbeitet mit externen, zertifizierten Spezialisten für Incident Response und IT-Forensik. (100 %) [https://www.weser-kurier.de/landkreis-verden/stadt-achim/cyberangriff-auf-achimer-stadtwerke-it-systeme-lahmgelegt-doc88feidafgmdhl0xoarw]

• Die Stadtwerke sprechen von einem „gezielten, kriminellen und professionellen Angriff“. (100 %) [https://www.butenunbinnen.de/nachrichten/cyberangriff-achim-stadtwerke-100.html]

• Die Zentralstelle Cybercrime Niedersachsen ermittelt und prüft einen Ransomware-Verdacht (berichtet, nicht vom Betreiber bestätigt). (100 %) [https://www.butenunbinnen.de/nachrichten/cyberangriff-achim-stadtwerke-100.html]

• Zu Angreifern, Erpressungsversuchen, Kontakt zu Tätern, Verhandlungen und Lösegeld äußert sich das Unternehmen während der laufenden Ermittlungen nicht. Externe Forensiker untersuchen Ursache und genaue Umstände. (100 %) [https://www.stadtwerke-achim.de/de/Unternehmen/Aktuelles/Wichtige-News/Wichtige-News_219387.html]

NICHT BEKANNT

• Einfallstor und Ursache

• Ob Daten verschlüsselt wurden

• Täter und Forderung

• Wann genau der erste Zugriff war (nur „Ende der Vorwoche“)

• Ob eine Gruppe den Angriff auf einer Leak-Site für sich beansprucht (bis 12.11. kein Eintrag gefunden)

WAHRSCHEINLICH (Einschätzung)

• Finanziell motivierter Angriff mit Erpressungsabsicht (Ransomware oder Datendiebstahl mit Drohung) (72 %) – Ermittler prüfen laut buten un binnen Ransomware; das Muster (Monitoring schlägt an, zentrale IT fällt aus, Isolation) entspricht Landsberg, Detmold und anderen Stadtwerke-Fällen. Kein Bekennerschreiben bekannt.

• Achim wurde nicht als politisches Ziel ausgesucht, sondern getroffen, weil ein Zugang möglich war (58 %) – Ransomware-Gruppen wählen Opfer meist nach Gelegenheit; „gezielt“ in der Betreibermeldung beschreibt eher die Professionalität. Ein staatlicher Hintergrund ist nicht auszuschließen, es gibt aber keinen Hinweis darauf.

• Die Angreifer waren schon einige Tage im Netz, bevor das Monitoring anschlug (62 %) – Das Unternehmen datiert den Angriff selbst auf „Ende der Vorwoche“, erkannt wurde er am Sonntag, 08.11.

2. Was ist die Auswirkung?

WISSEN

• Kundenportale (Kundenkonto, Zählerstandsübermittlung) sind nicht verfügbar, E-Mail ist derzeit nicht verfügbar. Telefonisch sind die Stadtwerke erreichbar, Anrufe werden dokumentiert. (100 %) [https://www.stadtwerke-achim.de/de/Unternehmen/Aktuelles/Wichtige-News/Wichtige-News_219387.html]

• Mails an den Kundenservice werden gesammelt und später weitergeleitet; Rückruf wird zugesagt. (100 %) [https://www.weser-kurier.de/landkreis-verden/stadt-achim/cyberangriff-auf-achimer-stadtwerke-it-systeme-lahmgelegt-doc88feidafgmdhl0xoarw]

• Strom, Gas und Fernwärme waren laut Betreiber zu keiner Zeit betroffen (Weser-Kurier nennt dazu auch Warmwasser). (100 %)
[https://www.stadtwerke-achim.de/de/Unternehmen/Aktuelles/Wichtige-News/Wichtige-News_219387.html]

• Laut Stadtwerken gibt es keine Anhaltspunkte, dass personenbezogene Daten abgeflossen sind; Experten halten eine Veröffentlichung für nicht wahrscheinlich, ein Darknet-Monitoring läuft. (100 %)
[https://www.stadtwerke-achim.de/de/Unternehmen/Aktuelles/Wichtige-News/Wichtige-News_219387.html]

• Kunden sollen bei unerwarteten Anrufen, E-Mails oder Nachrichten zu Energiethemen die Identität prüfen und keine sensiblen Daten herausgeben. (100 %)
[https://www.stadtwerke-achim.de/de/Unternehmen/Aktuelles/Wichtige-News/Wichtige-News_219387.html]

NICHT BEKANNT

• Ob doch Daten abgeflossen sind (Forensik läuft)

• Wie stark Abrechnung, Vertragswechsel und Messstellenbetrieb betroffen sind

• Ob Kundenzahlungen oder Lastschriften verzögert werden

WAHRSCHEINLICH (Einschätzung)

• Verzögerungen bei Abrechnung, Zählerstandsmeldungen und Vertragsänderungen (75 %) – Portale und zentrale IT sind isoliert; in Detmold und Landsberg zog sich das wochenlang.

• Betrüger nutzen den Vorfall für Phishing-Mails oder Anrufe (52 %) – Die Stadtwerke warnen selbst davor; das Muster ist nach öffentlichen Vorfällen verbreitet. Konkrete Fälle sind für Achim nicht berichtet.

• Daten wurden abgezogen (28 %) – Der Betreiber sieht derzeit keine Anhaltspunkte und hält eine Veröffentlichung laut Experten für unwahrscheinlich. Bei vielen Ransomware-Fällen zeigt sich Abfluss aber erst später.

3. Wie lange dauert es digital (Wiederherstellung IT)?

WISSEN

• Die Stadtwerke Achim nennen keinen Zeitpunkt für die Wiederherstellung. (100 %)
[https://www.stadtwerke-achim.de/de/Unternehmen/Aktuelles/Wichtige-News/Wichtige-News_219387.html]

• Detmold: Angriff Mitte November 2025, Telefon und E-Mail mehrere Wochen gestört, zum Jahreswechsel wieder voll verfügbar. (100 %)
[https://www.zfk.de/digitalisierung/hackerangriff-stadtwerke-detmold-kommunikation]

• Landsberg: Verschlüsselung in der Nacht zum 01.09.2026, Mitarbeiter danach nur eingeschränkt per Telefon und E-Mail erreichbar. (100 %)
[https://therecord.media/cyberattack-bavaria-germany-utility]

NICHT BEKANNT
• Ob funktionierende Offline-Backups vorhanden sind
• Ob Systeme neu aufgebaut werden müssen oder bereinigt werden können
• Reihenfolge der Wiederinbetriebnahme

WAHRSCHEINLICH (Einschätzung)
• Erste Dienste (E-Mail, einzelne Fachanwendungen) kommen innerhalb von ein bis drei Wochen zurück, der vollständige Normalbetrieb dauert mehrere Wochen bis etwa zwei Monate (63 %) – Entspricht Detmold (rund sechs Wochen) und anderen Stadtwerke-Fällen; ohne Wissen über Backups und Schadensumfang bleibt das eine Schätzung.
• Die Kundenportale bleiben länger offline als interne Systeme (55 %) – Internet-erreichbare Systeme werden nach Vorfällen meist zuletzt und erst nach Härtung wieder freigeschaltet; für Achim nicht belegt.

4. Ist in der Anlage etwas kaputt, das lange dauert?

WISSEN
• Laut Stadtwerken waren Strom, Gas und Fernwärme zu keiner Zeit betroffen; die Versorgung ist sicher und durchgehend. (100 %)
[https://www.stadtwerke-achim.de/de/Unternehmen/Aktuelles/Wichtige-News/Wichtige-News_219387.html]
• Laut buten un binnen fielen zentrale IT-Systeme und Kundenportal aus, von Anlagen ist keine Rede. (100 %) [https://www.butenunbinnen.de/nachrichten/cyberangriff-achim-stadtwerke-100.html]

NICHT BEKANNT
• Wie Büro-IT und Leittechnik/Fernwirktechnik bei den Stadtwerken getrennt sind
• Ob die Trennung aller Außenverbindungen Fernwartung, Zählerfernauslesung oder Dienstleister-Zugänge betrifft
• Ob Angreifer Kontakt zu OT-Systemen hatten

WAHRSCHEINLICH (Einschätzung)
• Physische Anlagen wie Trafostationen, Gasdruckregelanlagen oder Heizwerke sind nicht beschädigt (85 %) – Der Betreiber meldet durchgehende Versorgung; bei Stadtwerke-Ransomware in DACH sind bisher keine Anlagenschäden öffentlich belegt.
• Der Betrieb läuft mit mehr Handarbeit, etwa bei Störungsannahme, Einsatzplanung oder Messwerten (45 %) – Typisch, wenn Büro-IT isoliert ist; für Achim nicht berichtet.

5. Wie viele solcher Ziele gibt es?

WISSEN
• Der VKU hatte am 09.07.2025 rund 1.600 Mitgliedsunternehmen (Energie, Wasser, Abfall, Telekommunikation). (100 %)
[https://www.vku.de/fileadmin/user_upload/Verbandsseite/Publikationen/2025/VKU_ZDF_2025_DE.pdf]
• Das NIS2-Umsetzungsgesetz gilt seit 06.12.2025; rund 29.500 Unternehmen müssen sich beim BSI registrieren (Sekundärquelle, BSI-Original nicht geprüft). (100 %)
[https://www.pv-magazine.de/2026/01/06/bsi-schaltet-portal-fuer-nis-2-registrierung-frei/]
• Stadtwerke Detmold: Angriff Mitte November 2025. (100 %) [https://heise.de/-11083097]
• Vereinigte Stadtwerke: Angriff Mitte November 2025 über einen IT-Dienstleister, teilweiser Datenabfluss von einem Server (Pressemitteilung 27.11.2025); Leak-Site-Eintrag der Gruppe Payoutsking am 14.01.2026 (Drittquelle). (100 %) [https://borncity.com/blog/?p=319692]
• Stadtwerke Landsberg: Verschlüsselung der zentralen IT ab Nacht zum 01.09.2026. (100 %)
[https://therecord.media/cyberattack-bavaria-germany-utility]
• GSW Gemeinschaftsstadtwerke (Kamen): Leak-Site-Eintrag der Gruppe Qilin 2026 (Drittquelle, berichtet). (100 %)
[https://cyberthreatintelligence.net/ransomware-victim/gsw-gemeinschaftsstadtwerke-gmbh-qilin-2026]

• Laut BSI gehört die Energiebranche weiterhin zu den am stärksten angegriffenen KRITIS-Sektoren, oft über ausgenutzte Schwachstellen. (100 %)

[https://www.zfk.de/digitalisierung/it/bsi-lagebericht-energiebranche-bleibt-angriffsziel]

• Shodan (aggregiert): OT-Protokolle öffentlich erreichbar in Deutschland: 140110 gesamt (DNP3 31683, OMRON FINS 26391, ProConOS 15525, EtherNet/IP 15295, Siemens S7 7580, OPC UA 4964) (100 %)

NICHT BEKANNT

• Eine amtliche Zahl erfolgreicher Angriffe auf Stadtwerke pro Jahr ist öffentlich nicht verfügbar

• Wie viele Stadtwerke sich tatsächlich beim BSI registriert haben

WAHRSCHEINLICH (Einschätzung)

• Die tatsächliche Zahl erfolgreicher Angriffe auf Stadtwerke liegt über den öffentlich bekannten Fällen (70 %) – Nicht jeder Vorfall wird öffentlich; Leak-Site-Einträge tauchen oft ohne Pressemeldung auf.

6. Kann das wieder passieren?

WISSEN

• Laut BSI-Lagebericht 2025 sind professionell organisierte Ransomware-Gruppen weiter die größte Bedrohung (Sekundärquelle). (100 %)

[https://der-betrieb.de/meldungen/bsi-lagebericht-2025-hacker-finden-weiter-leichtes-spiel/]

• Bei den Stadtwerken Neumünster zeigte die Aufarbeitung des Angriffs 2023, dass es schon 2016 einen ähnlichen Angriff gegeben hatte. (100 %)

[https://www.zfk.de/digitalisierung/boeddeker-die-hacker-haben-sich-immer-weiter-vorgetastet]

NICHT BEKANNT

• Ob das Einfallstor bei Achim schon geschlossen ist

• Ob Zugangsdaten im Umlauf sind

WAHRSCHEINLICH (Einschätzung)

• Weitere Stadtwerke in Deutschland werden in den nächsten Monaten erfolgreich angegriffen (90 %) – Kontinuierliche Fallserie 2025 bis 2026, Lage laut BSI unverändert angespannt.

• Achim selbst wird kurzfristig erneut erfolgreich angegriffen (15 %) – Nach einem Vorfall wird meist neu aufgebaut und gehärtet; Wiederholungsangriffe kommen vor, sind aber nicht die Regel.

Lage

Die Monitoring-Systeme der Stadtwerke Achim haben am Sonntag, 8. November 2026, einen Angriff erkannt, der laut Unternehmen Ende der Vorwoche stattfand. Zentrale IT-Systeme, Kundenportale und E-Mail sind ausgefallen, die Stadtwerke haben alle Außenverbindungen getrennt. Strom, Gas und Fernwärme sind laut Betreiber nicht betroffen. Die Zentralstelle Cybercrime Niedersachsen ermittelt und prüft laut buten un binnen einen Ransomware-Verdacht. Bis heute hat sich kein Täter öffentlich bekannt.

Angriff	Angriff auf zentrale IT-Systeme; Kundenportale und E-Mail ausgefallen, IT isoliert, alle Außenverbindungen getrennt. Ermittler prüfen Ransomware-Verdacht.
Wann / Status	Laut Unternehmen Ende der Woche vor dem 08.11.2026; erkannt am 08.11.2026 · eingedämmt
Täter	unbekannt; bis 12.11.2026 kein Leak-Site-Eintrag gefunden – unbekannt
Betreiber / Branche	Stadtwerke Achim AG · Energieversorgung (Strom, Gas, Fernwärme, Warmwasser)
Anlage / Alter	kommunaler Versorger; Büro-IT, Kundenportale betroffen, Anlagen laut Betreiber nicht ·

Region	Achim, Landkreis Verden, Niedersachsen; Versorgungsgebiet laut Stellenanzeige Achim, Oyten, Langwedel, Ottersberg
Auswirkungen	Versorgung mit Strom, Gas und Fernwärme laut Betreiber durchgehend gesichert. Für Kunden: kein Kundenportal, keine Online-Zählerstandsmeldung, keine E-Mail; Telefon funktioniert. Datenabfluss laut Betreiber derzeit ohne Anhaltspunkte, Darknet-Monitoring läuft.
Behörden	BSI; Landesbeauftragter für den Datenschutz Niedersachsen (Meldung nach Art. 33 DSGVO); Polizei/LKA, laut buten un binnen ermittelt die Zentralstelle Cybercrime Niedersachsen.
Regulatorik	NIS2: Seit 06.12.2025 gilt das NIS2UmsuCG; Energieversorger dieser Größe fallen nach den Schwellen (ab 50 Beschäftigte oder über 10 Mio. Euro Umsatz) mindestens als wichtige Einrichtung darunter (Einstufung für Achim vermutet, nicht geprüft). Meldepflicht an das BSI: Frühwarnung in 24 Stunden, Meldung in 72 Stunden, Abschlussbericht nach einem Monat. KRITIS-Schwellen der BSI-KritisV werden bei rund 45.000 Kunden vermutlich nicht erreicht (vermutet). Falls die Stadtwerke Netzbetreiber sind, gilt der IT-Sicherheitskatalog der BNetzA nach § 11 EnWG (nicht geprüft). DSGVO: Meldung nach Art. 33 ist erfolgt, Benachrichtigung Betroffener nach Art. 34 bei hohem Risiko angekündigt. CRA betrifft Hersteller, für diesen Fall nicht direkt relevant.

Angriffsvektor

Noch nicht bekannt – Hypothesen (Einschätzung):

• Ausgenutzte Schwachstelle in Edge Devices (VPN-Gateway, Firewall, Remote Access) (hoch): Laut BSI ist Ausnutzen offener Schwachstellen ein Hauptweg in die Energiebranche (zfk, BSI-Lagebericht); Edge Devices waren 2025/2026 das häufigste Einfallstor bei Ransomware. Für Achim nicht belegt.

• Gestohlene oder erratene Zugangsdaten für Fernzugänge, eventuell von einem Initial Access Broker gekauft (mittel): Verbreitet bei mittelgroßen Organisationen ohne durchgängige Mehrfaktor-Anmeldung. Hinweis: Die Massen-Anmeldeversuche 2024 betrafen die Stadtverwaltung Achim, nicht die Stadtwerke (Weser-Kurier 04.12.2024), daraus lässt sich nichts ableiten.

• Phishing mit Malware als Erstzugang (mittel): Klassischer Weg bei Ransomware, nach wie vor häufig; keine Hinweise im Fall Achim.

• Zugang über einen IT-Dienstleister (gering): Bei den Vereinigten Stadtwerken 2025 der Weg; in Achim spricht der Betreiber von keinen betroffenen Partner- oder Kundensystemen.

Zeitleiste

04.12.2024 Weser-Kurier berichtet über abgewehrte Massen-Anmeldeversuche auf die Stadtverwaltung Achim (andere Organisation, kein belegter Zusammenhang) – berichtet [https://www.weser-kurier.de/landkreis-verden/stadt-achim/cyberkriminelle-nehmen-achimer-stadtverwaltung-ins-visier-doc7yc2nilk6o41833ilmu4]

Ende der Woche vor dem 08.11.2026 Angriff findet laut Unternehmen statt – bestätigt [https://www.weser-kurier.de/landkreis-verden/stadt-achim/cyberangriff-auf-achimer-stadtwerke-it-systeme-lahmgelegt-doc88feidafgmdhl0xoarw]

08.11.2026 (Sonntag) Monitoring erkennt den Angriff, zentrale IT fällt aus, Isolation und Trennung der Außenverbindungen – bestätigt [https://www.stadtwerke-achim.de/de/Unternehmen/Aktuelles/Wichtige-News/Wichtige-News_219387.html]

bis 11.11.2026 BSI, Landesdatenschutzbeauftragter (Art. 33 DSGVO) und Polizei informiert – bestätigt [https://www.stadtwerke-achim.de/de/Unternehmen/Aktuelles/Wichtige-News/Wichtige-News_219387.html]

11.11.2026 Meldung auf der Website der Stadtwerke; Weser-Kurier berichtet um 17:14 Uhr – bestätigt [https://borncity.com/blog/2026/11/12/sicherheits-news-vom-12-11-2026/]

12.11.2026 buten un binnen: Zentralstelle Cybercrime Niedersachsen ermittelt, Ransomware-Verdacht – berichtet
[https://www.butenunbinnen.de/nachrichten/cyberangriff-achim-stadtwerke-100.html]

Vergleichsfälle

• Stadtwerke Detmold (2025): Telefon und E-Mail waren mehrere Wochen gestört, die Netzsteuerung lief stabil weiter.
[https://www.zfk.de/digitalisierung/hackerangriff-stadtwerke-detmold-kommunikation]

• Vereinigte Stadtwerke (2025): Der Weg führte über einen IT-Dienstleister, Daten flossen von einem Server ab, Monate später tauchte ein Leak-Site-Eintrag auf. [https://borncity.com/blog/?p=319692]

• Stadtwerke Landsberg (2026): Zentrale IT verschlüsselt, Versorgung unberührt, ein Abfluss von Kundendaten ließ sich nicht ausschließen. [https://therecord.media/cyberattack-bavaria-germany-utility]

• Stadtwerke Neumünster (2023): Die Forensik fand Spuren eines früheren Angriffs aus 2016, gründliche Aufarbeitung lohnt sich.
[https://www.zfk.de/digitalisierung/boeddeker-die-hacker-haben-sich-immer-weiter-vorgetastet]

Begriffe einfach erklärt

OT: Operational Technology, also die Technik, die Netze, Pumpen und Heizwerke steuert, im Unterschied zur Büro-IT.

Ransomware: Schadsoftware, die Daten verschlüsselt, damit die Täter Lösegeld fordern können.

Incident Response: Die geordnete Reaktion auf einen Angriff: eindämmen, untersuchen, wiederherstellen.

Forensik: Spurensuche in Computern, um herauszufinden, wie und wann die Angreifer hereinkamen.

Segmentierung: Das Aufteilen von Netzen, damit ein Angriff im Büro nicht bis zur Anlagensteuerung durchkommt.

NIS2: EU-Regeln für Cybersicherheit, die seit Dezember 2025 auch in Deutschland für viele Versorger gelten.

Früherer Stand: Erstmeldung (11.11.2026 18:00)

Wissen 33 % · wahrscheinlich 27 % · nicht bekannt 40 %
Die Stadtwerke Achim haben am Sonntag, 8. November 2026, über ihr Monitoring einen Cyberangriff erkannt, der laut Unternehmen schon Ende der Vorwoche stattfand. Zentrale IT-Systeme sind ausgefallen, die Kundenportale sind nicht erreichbar, E-Mails sind gestört, und alle Außenverbindungen wurden getrennt. Strom, Gas, Fernwärme und Warmwasser sind laut Stadtwerken nicht betroffen; über Täter, Forderungen und den Angriffsweg sagt das Unternehmen mit Verweis auf die laufende Forensik nichts.

Öffentliche Einschätzung von OT-Cyber auf Basis öffentlicher Quellen. Prozent = Einschätzung: 100 % bestätigt, 0 % sicher falsch. Fachliche Einschätzung, keine Schuldzuweisung.