

WOCHENBERICHT

OT-/Cyber-Lagebild Kommunale Versorger und KRITIS

Ausgabe KW 43/2026 · Kommunale Versorger und KRITIS in DACH

Zielgruppe	Stadtwerke, Wasser- und Abwasserbetriebe, KRITIS-Betreiber
Berichtszeitraum	16.10.2026–23.10.2026
Version	1.0
Datum	23.10.2026
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

Rund um den Berichtszeitraum (15. bis 23.10.) wurden aktiv ausgenutzte Schwachstellen in Fernwartung und Edge Devices veröffentlicht, vor allem bei BeyondTrust und VeloCloud. Sie betreffen Systeme, die bei Stadtwerken die Brücke zwischen Internet und Leittechnik bilden. Am schwersten wiegt BeyondTrust Remote Support (CVE-2026-102764): Die Lücke wurde vor der Veröffentlichung ausgenutzt; die zwei bekannten Kompromittierungen datiert BeyondTrust auf den 29.08. Laut Rapid7 ordnet Mandiant die Aktivität aus seiner Untersuchung der mutmaßlich China-nahen Spionagegruppe ARMORY CASTLE (früher UNC5221) zu, seit dem 16.10. steht die Lücke im KEV-Katalog. Laut Rapid7 rät Mandiant, vor Änderungen Beweise zu sichern, verdächtige Appliances zu isolieren und sie aus einem sauberen, gepatchten Image neu aufzubauen, wenn eine Kompromittierung bestätigt ist oder sich nicht ausschließen lässt. Dazu kommen ein neuer Zero-Day im VeloCloud Orchestrator (SD-WAN zu Außenstellen) und PHP2Shell. Für diese zwei kritischen RCE-Lücken in PHP sind Notfall-Patches erschienen.

In der Leittechnik meldet Siemens acht CVEs (Typen laut CISA: Eval Injection und Cross-Site Scripting) im Webserver von S7-1500 und ET 200SP, für einen großen Teil der Produkte noch ohne Fix (CVSS bis 9,6); Siemens bereitet Fixes vor und empfiehlt bis dahin Gegenmaßnahmen. Angreifer können damit SPS-Operationen im Rahmen der Rechte des angemeldeten Nutzers ausführen. Die Eclipse-Milo-Lücken im OPC-UA-Stack betreffen laut CISA ausdrücklich Wasser und Abwasser. Das gemeinsame SafePay-Advisory von FBI, CISA, US Secret Service, LKA Rheinland-Pfalz sowie der britischen National Crime Agency und der North West Regional Organised Crime Unit nennt als Einstieg gestohlene oder erratene Passwörter, ausgenutzte Schwachstellen und Phishing. Für kleine Teams heißt das: zuerst Secure Remote Access (CC4) und risikobasiertes Vulnerability Management (CC5), danach Visibility (CC3) an der Grenze zwischen IT und OT.

GESAMTBEWERTUNG

Die Lage ist hoch. Vorrang haben Fernwartungs- und VPN-Zugänge (BeyondTrust, VeloCloud, VPN ohne MFA): patchen, auf Kompromittierung prüfen und hinterlegte Zugangsdaten wechseln.

Trends

- Spionagegruppen wie ARMORY CASTLE, laut Rapid7 von Mandiant als mutmaßlich China-nah eingeordnet, und Ransomware-Gruppen zielen gezielt auf Fernwartungs- und Management-Systeme (BeyondTrust, VeloCloud, FortiManager), weil diese mit einem Einbruch Zugangsdaten für viele nachgelagerte Systeme liefern.
- Patches allein reichen oft nicht: Rapid7 empfiehlt, auch nach dem Patch auf Kompromittierung zu prüfen, deshalb gehört ein Compromise Assessment zum Standard.
- Angriffe auf die Lieferkette der Leittechnik nehmen zu, über Software-Bibliotheken (Eclipse Milo), Hersteller-CRM (Loxone) und von Angreifern per ClickFix-Köder mitgebrachte, echt signierte Hersteller-Tools (Siemens Software Center).
- Bei der Leittechnik kommen Advisories, für die es noch keinen Fix gibt (S7-1500 Webserver), häufiger vor, dann schützt nur eine gute Architektur.

Lageübersicht

ID	Meldung	Relevanz	Quelle
L-01	BeyondTrust Remote Support: vor der Veröffentlichung ausgenutzt, seit 16.10. im KEV (CVE-2026-102764)	KRITISCH	Rapid7 / BleepingComputer (Mandiant, GTIG, CISA KEV), 16.10.
L-02	Siemens SIMATIC S7-1500 und ET 200SP: acht CVEs im Webserver, für einen großen Teil der Produkte noch kein Fix (ICSA-26-295-14)	HOCH	CISA ICS Advisory, 22.10.
L-03	PHP2Shell: kritische RCE-Lücken in PHP (CVE-2026-109618/-109619)	HOCH	BleepingComputer, 21.10.
L-04	SafePay-Ransomware: gemeinsames Advisory von FBI, CISA, US Secret Service, LKA Rheinland-Pfalz und britischen Behörden (AA26-293A)	HOCH	CISA Cybersecurity Advisory, 20.10.
L-05	Arista VeloCloud Orchestrator: neuer Zero-Day, Konto mit Basisrechten reicht (CVE-2026-114625)	HOCH	BleepingComputer, 22.10.
L-06	Eclipse Milo (OPC UA): sechs CVEs (der Kopf des CISA-Advisorys nennt fünf), kein Patch für 0.6.x (ICSA-26-288-01)	HOCH	CISA ICS Advisory, 15.10.
L-07	Loxone: Cyberangriff auf CRM und Partnerdaten, laut Loxone weltweit keine Vorkommnisse bei Kundeninstallationen	MITTEL	Loxone-Sicherheitsseite, 19.10.

Exponierte OT-Systeme (Shodan)

Exponierte OT-Systeme (Shodan, Stand 23.10.2026):

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	144393	DNP3: 33922, OMRON FINS: 24335, ProConOS: 16607, Siemens S7: 8039, OPC UA: 5548
Österreich	4715	HMI/VNC: 1070, DNP3: 969, IEC-104: 455, Siemens S7: 365, OPC UA: 141

Meldungen im Detail

L-01 BeyondTrust Remote Support: vor der Veröffentlichung ausgenutzt, seit 16.10. im KEV (CVE-2026-102764)

KRITISCH Rapid7 / BleepingComputer (Mandiant, GTIG, CISA KEV), 16.10.

Was ist neu: BeyondTrust hat die Authentication Bypass Lücke am 15.10. veröffentlicht, CISA hat sie am 16.10. in den KEV-Katalog aufgenommen. Die Lücke wurde vor der Veröffentlichung ausgenutzt; die zwei bekannten Kompromittierungen datiert BeyondTrust auf den 29.08.2026, eine gehostete Instanz und eine selbst betriebene Appliance. Laut Rapid7 ordnet Mandiant die Aktivität aus seiner Untersuchung der mutmaßlich China-nahen Spionagegruppe ARMORY CASTLE (früher UNC5221) zu. Die Gruppe legt eine PHP-Webshell und den Tunneler BARECLAW ab, versucht den Credential Vault auszulesen und löscht Logs. Betroffen sind laut Rapid7 Versionen 26.2.3 und älter, sofern der Patch BT26-05-RS nicht eingespielt ist.

Bedeutung: Wo BeyondTrust als Fernwartungszugang für Leittechnik-Dienstleister genutzt wird, liegen auf der Appliance oft Zugangsdaten zu OT-Jump-Hosts. Mandiant beobachtete den Versuch, den Credential Vault auszulesen. Laut Rapid7 sollten gespeicherte oder vermittelte Zugangsdaten nach Patch oder Neuaufbau gewechselt und administrative Änderungen geprüft werden. Rapid7 empfiehlt außerdem, auch nach dem Patch auf Kompromittierung zu prüfen.

Empfehlung: Selbst betriebene Appliances sofort patchen und anhand der IoCs von Mandiant und Rapid7 prüfen. Alle im Vault hinterlegten Zugangsdaten wechseln und die Fernwartung bis dahin nur mit Freigabe im Einzelfall öffnen (CC4).

Quelle: <https://www.rapid7.com/blog/post/etr-cve-2026-102764-critical-beyondtrust-remote-support-authentication-bypass-exploited-in-the-wild/> ✓ geprüft

L-02 Siemens SIMATIC S7-1500 und ET 200SP: acht CVEs im Webserver, für einen großen Teil der Produkte noch kein Fix (ICSA-26-295-14)

HOCH CISA ICS Advisory, 22.10.

Was ist neu: CVE-2026-63350 bis -63357 betreffen den Webserver von S7-1500, ET 200SP, Drive Controllern, Open und Software Controllern sowie PLCSIM Advanced in allen Versionen. Die Lücken ermöglichen Angriffe im Browser des Nutzers (Cross-Site Scripting): Ein Angreifer kann Schadcode in der Browsersitzung eines berechtigten Nutzers ausführen und mit dessen Rechten Aktionen auf der SPS durchführen. Siemens rät u. a., nur vertrauenswürdige Trace-Dateien hochzuladen. Für einen großen Teil der Produkte gibt es noch keinen Fix; Siemens bereitet Fixes vor und empfiehlt bis dahin Gegenmaßnahmen.

Bedeutung: Die S7-1500 ist eine weit verbreitete SPS-Familie, auch in der Wasser- und Fernwärmeautomatisierung im DACH-Raum. Der Webserver ist im Feld oft aus Bequemlichkeit eingeschaltet. Weil es für einen großen Teil der Produkte noch keinen Fix gibt, schützt bis dahin nur die Konfiguration.

Empfehlung: Im Asset-Inventar alle S7-1500 und ET 200SP mit aktivem Webserver finden. Den Webserver abschalten, wo er nicht gebraucht wird, sonst den Zugriff per Firewall auf Engineering-Netze beschränken. Nur vertrauenswürdige Trace-Dateien hochladen (CC2).

Quelle: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-295-14> ✓ geprüft

L-03 PHP2Shell: kritische RCE-Lücken in PHP (CVE-2026-109618/-109619)

HOCH BleepingComputer, 21.10.

Was ist neu: Zwei kritische Lücken in PHP selbst erlauben Remote Code Execution (CVSS 4.0 je 9,2). Notfall-Patches sind mit PHP 8.5.12, 8.4.27, 8.3.36 und 8.2.35 erschienen. Für 7.4, 8.0 und 8.1 hat das PHP-Team ausnahmsweise minimale Source-Backports bereitgestellt. Das britische NCSC rät, betroffene Systeme sofort zu aktualisieren oder bis zum Patch vom Netz zu nehmen.

Bedeutung: Kundenportale, Webseiten und Störungsmelder von Stadtwerken laufen oft auf PHP-Systemen wie WordPress, TYPO3, Drupal oder Nextcloud, häufig beim kommunalen Rechenzentrum. Ein Update von WordPress oder TYPO3 behebt das Problem nicht, nur das Update der PHP-Laufzeit hilft.

Empfehlung: Alle eigenen und beim Dienstleister gehosteten PHP-Server erfassen und den PHP-Stand schriftlich bestätigen lassen. Für PHP 8.1 und älter beim Distributor nach Backports fragen oder migrieren. Webserver in der DMZ halten, ohne Route ins OT-Netz (CC5).

Quelle:

<https://www.bleepingcomputer.com/news/security/php-ships-emergency-patches-for-critical-php2shell-flaws/>

✓ geprüft

L-04 SafePay-Ransomware: gemeinsames Advisory von FBI, CISA, US Secret Service, LKA Rheinland-Pfalz und britischen Behörden (AA26-293A)

HOCH CISA Cybersecurity Advisory, 20.10.

Was ist neu: Seit August 2024 sind mindestens 600 Organisationen aus mehreren Sektoren kritischer Infrastruktur von SafePay betroffen, auch in Europa. Der Einstieg erfolgt laut Advisory über gestohlene oder erratene Passwörter, ausgenutzte Schwachstellen und Phishing; genannt werden u. a. CVE-2020-3259, CVE-2023-20269, CVE-2023-27532, CVE-2024-40711 und CVE-2024-40766. Die Akteure schalten Sicherheitsfunktionen ab, um unentdeckt zu bleiben. Herausgeber sind FBI, CISA, US Secret Service, LKA Rheinland-Pfalz sowie die britische National Crime Agency und die North West Regional Organised Crime Unit; das Advisory stützt sich auf Ermittlungen von FBI, USSS und LKA Rheinland-Pfalz.

Bedeutung: Nach unserer Einordnung betreffen die CVEs u. a. VPN-Systeme und Veeam Backup, das Advisory nennt keine Hersteller. Dass ein deutsches LKA an den Ermittlungen beteiligt ist, zeigt den Bezug zu DACH. Wenn das Backup ausfällt, verlängert das den Ausfall der kaufmännischen IT und damit auch der Abrechnung und Leitstellen-IT.

Empfehlung: Alle fünf CVEs gegen das Asset-Inventar prüfen und MFA an allen VPN- und Webmail-Zugängen nachweisen. Mindestens eine Backup-Kopie unveränderlich und offline halten und die Wiederherstellung testen. Den IR-Plan um das Szenario „Sicherheitsfunktionen abgeschaltet“ ergänzen (CC1).

Quelle: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-293a> ✓ geprüft

L-05 Arista VeloCloud Orchestrator: neuer Zero-Day, Konto mit Basisrechten reicht (CVE-2026-114625)

HOCH BleepingComputer, 22.10.

Was ist neu: Arista hat einen weiteren Zero-Day im VeloCloud Orchestrator geschlossen, der bereits ausgenutzt wird. Schon ein Nutzer mit Basisrechten (basic privileges) und gültiger Sitzung auf der VCO-Weboberfläche kann ihn ohne weitere Interaktion ausnutzen und sich höhere Rechte verschaffen. Schon im Juli wurde eine andere VCO-Lücke ausgenutzt (CVE-2026-16812).

Bedeutung: Wer über VeloCloud Außenstellen anbindet, macht den Orchestrator zur zentralen Steuerstelle für die Wege ins Fernwirknetz. Wer dort höhere Rechte erlangt, kann Routen und Tunnel zu Außenstellen verändern.

Empfehlung: Patch einspielen und die Weboberfläche des Orchestrators nur aus dem Management-Netz erreichbar machen. Konten mit niedrigen Rechten prüfen und Admin-Änderungen seit Juli in den Logs nachvollziehen (CC4).

Quelle: <https://www.bleepingcomputer.com/news/security/arista-patches-new-velocloud-orchestrator-zero-day-exploited-in-attacks/> ✓ geprüft

L-06 Eclipse Milo (OPC UA): sechs CVEs (der Kopf des CISA-Advisorys nennt fünf), kein Patch für 0.6.x (ICSA-26-288-01)

HOCH CISA ICS Advisory, 15.10.

Was ist neu: Betroffen sind Eclipse Milo 0.6.0 bis 1.1.4. Die Lücken können dazu führen, dass der Server nicht mehr antworten kann (Denial of Service, CVE-2026-63252), und erlauben Methodenaufrufe sowie das Löschen von Knoten durch anonyme Clients (CVE-2026-58080, CVSS v3.1 8,2). Über ein Padding Oracle lassen sich Passwörter zurückgewinnen (CVE-2026-60007, CVSS v4 9,1). Behoben ab Version 1.1.5; für 0.6.x gibt es keinen Fix. Der Kopf des Advisories nennt 5 Lücken, im Text stehen 6 CVEs.

Bedeutung: CISA nennt die Sektoren Chemie, kritische Fertigung, Energie sowie Wasser und Abwasser. Milo steckt als Java-Bibliothek in Produkten, ohne dass der Betreiber davon weiß. Ohne SBOM fällt das im Asset-Inventar nicht auf.

Empfehlung: Die Hersteller von SCADA, Gateways und Edge-Geräten schriftlich fragen, ob Milo verbaut ist und wann ein Update kommt. Anonyme OPC-UA-Zugriffe abschalten und OPC-UA-Verkehr im OT-Monitoring sichtbar machen (CC5, CC3).

Quelle: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-288-01> ✓ geprüft

L-07 Loxone: Cyberangriff auf CRM und Partnerdaten, laut Loxone weltweit keine Vorkommnisse bei Kundeninstallationen

MITTEL Loxone-Sicherheitsseite, 19.10.

Was ist neu: Loxone meldet einen Cyberangriff auf interne Unternehmenssysteme, insbesondere CRM-Systeme mit Daten der Partnerbetriebe sowie Bewerberdaten. Laut Loxone gibt es weltweit keine Vorkommnisse bei Kundeninstallationen und keinen Zugriff auf Kundeninstallationen. Externe IT-Sicherheits- und Forensikexperten sind eingebunden. Loxone führt Zwei-Faktor-Authentifizierung ein.

Bedeutung: Nach unserer Einschätzung lassen sich mit gestohlenen Daten der Installateure glaubwürdige Phishing-Mails an Betreiber kommunaler Gebäude und Bäder schreiben, angeblich vom eigenen Elektriker. Laut Loxone gibt es weltweit keine Vorkommnisse bei Kundeninstallationen und keinen Zugriff auf Kundeninstallationen.

Empfehlung: Rückfragen bei Mails zu Updates oder Fernzugriff auf Loxone-Anlagen immer über eine bekannte Telefonnummer klären. Prüfen, welche Miniserver aus dem Internet erreichbar sind, und die Zugangsdaten dort ändern (CC4).

Quelle: <https://security.loxone.com/dede/> ✓ geprüft

Empfehlungen

Nr.	Maßnahme	Bezug	Priorität	Zeitraum
M-01	BeyondTrust-Appliance patchen, Compromise Assessment durchführen und alle hinterlegten Zugangsdaten zu OT-Systemen wechseln [CC4 Secure Remote Access]	L-01	HOCH	sofort
M-02	Webserver der S7-1500 und ET 200SP abschalten oder per Firewall auf Engineering-Netze beschränken, bis Siemens Fixes liefert [CC2 Defensible Architecture]	L-02	HOCH	sofort
M-03	MFA an allen VPN-Zugängen erzwingen und bekannte Lücken in Edge Devices sowie in VeloCloud und PHP-Webservern risikobasiert vor allem anderen schließen [CC5 Risk-Based Vulnerability Management]	L-04	HOCH	sofort
M-04	SBOM von SCADA-, Gateway- und Edge-Herstellern einfordern und OPC-UA-Verkehr im OT-Monitoring sichtbar machen [CC3 ICS Network Visibility & Monitoring]	L-06	MITTEL	0 bis 3 Monate
M-05	IR-Plan um die Szenarien „kompromittierte Fernwartung“ und „Sicherheitsfunktionen abgeschaltet“ ergänzen und einmal als Tabletop üben [CC1 ICS Incident Response]	L-04	MITTEL	0 bis 3 Monate

Fragen für das nächste Jour fixe

1. Welche Fernwartungslösungen (BeyondTrust, TeamViewer, VPN) nutzen unsere Leittechnik-Dienstleister, und wer hat sie seit August auf Kompromittierung geprüft?
2. Auf welchen S7-1500 und ET 200SP ist der Webserver aktiv, und wer braucht ihn wirklich?

3. Haben unsere SCADA- und Gateway-Hersteller eine SBOM geliefert, und steckt Eclipse Milo darin?
4. Hat unser kommunales Rechenzentrum PHP auf allen Portalen und Webseiten aktualisiert, und haben wir das schriftlich?
5. Ist MFA an jedem VPN-Zugang nachweisbar aktiv, auch für Dienstleister und Notfallkonten?

Maßnahmen dieser Woche

1. BeyondTrust Remote Support: Patch BT26-05 prüfen, IoCs von Mandiant und Rapid7 abgleichen und alle im Vault gespeicherten OT-Zugangsdaten wechseln.
2. VeloCloud Orchestrator On-Prem auf 5.2.3.18, 6.1.3.10 oder 6.4.2.12 bringen und die Weboberfläche auf das Management-Netz beschränken.
3. Liste aller S7-1500 und ET 200SP mit aktivem Webserver erstellen, nicht benötigte Webserver abschalten und Ports 80/443 an der Zellen-Firewall sperren.
4. PHP-Stand aller Webserver (eigene und beim Dienstleister) auf 8.2.35, 8.3.36, 8.4.27 oder 8.5.12 prüfen lassen.
5. Die fünf CVEs aus dem SafePay-Advisory gegen das Asset-Inventar laufen lassen und MFA am VPN für alle Konten nachweisen.
6. Windows- und Engineering-PCs auf ClickFix- und MSI-Ausführungen prüfen. Laut The Hacker News bringen die Angreifer eine echte, signierte ältere Kopie (laut Siemens war 3.5.8.7 damals aktuell) samt archive.dll per MSI über einen ClickFix-Köder selbst mit. Siemens empfiehlt das Update auf 4.0.9.8; laut The Hacker News empfiehlt der Siemens-Hinweis außerdem, die IoCs zu sperren und nach einer SiemensSoftwareCenter.exe in AppData\Local\Programs zu suchen, die von msixexec.exe gestartet wurde.

HINWEIS ZUR QUELLENLAGE

Für Siemens S7-1500, Eclipse Milo, SafePay und Loxone liegen Primärquellen vor (CISA, Hersteller). BeyondTrust, VeloCloud und PHP2Shell sind über mehrere Fachquellen belegt, die CVSS-Werte weichen dort aber voneinander ab. Nicht aufgenommen, weil nicht unabhängig bestätigt: WAGO ICSA-26-293-02 / VDE-2026-096 (CISA-Seite liefert 404, CERT@VDE nicht gefunden), die Nennung von „utilities and energy“ bei PAN-OS CVE-2026-0257 (nur Sekundärquellen, Unit 42 nicht direkt geprüft), die Behauptung einer Leak-Site über einen deutschen Kläranlagenbauer (nur Angaben der Täter, widersprüchliche Daten) und die Täterangaben „Samurai“ und 300.000 Seriennummern zum Loxone-Leak. In DACH fanden wir für den Zeitraum keinen bestätigten Vorfall bei einem Wasser- oder Abwasserbetrieb. Alle Quellenlinks wurden am 23.10.2026 automatisch aufgerufen und inhaltlich geprüft. Am 23.10.2026 nach dem Qualitäts-Tor zusätzlich gegen Primärquellen geprüft (CISA, Rapid7/Mandiant, Unit 42, Loxone, Siemens) und korrigiert; nicht belegte Angaben wurden gestrichen.