

L A G E B I L D

OT-/Cyber-Lagebild

Ausgabe 15.10.2026, 16:18 Uhr · Betreiber und Maschinenbauer in Bayern, Salzburg, Tirol und ganz DACH

Zielgruppe	Stadtwerke, Wasser- und Energieversorger, Industrie, Maschinenbau, KRITIS
Datum	15.10.2026
Herausgeber	Maximilian Gilg, OT-Cyber.de, Rosenheim
Klassifizierung	TLP:CLEAR – ausschließlich öffentliche Quellen
Online	https://ot-cyber.de/ot-lage/

Dieses Lagebild fasst öffentlich zugängliche Meldungen zusammen – automatisch zusammengestellt, ohne Gewähr. Die Relevanz bezieht sich auf Betreiber von Anlagen und Maschinen in Deutschland, Österreich und der Schweiz.

Management Summary

Diese Ausgabe enthält 11 Meldungen, davon 4 mit hoher Relevanz für Betreiber in DACH.

- ****Palo Alto PAN-OS: Lücke in der Management-Oberfläche wird bereits ausgenutzt (CVE-2026-0322, CVSS 4.0: 8,6, 14.10.)****
- ****Nachtrag Moxa MGate MB3170/MB3270: zwei schwere Lücken in Modbus-Gateways (CVE-2026-86325, CVSS 4.0: 9,4; CVE-2026-86326: 8,6)****
- ****Cybervorfall beim Baukonsortium des Fehmarnbelt-Tunnels (13.10.)****
- ****SOCRadar meldet: Initial Access Broker „CyberXero“ soll ukrainische Energieunternehmen ausgespäht und Kundendaten gestohlen haben (Bericht vom 06.10., Medien seit 12.10.)****

GESAMTBEWERTUNG

Hoch – vorrangig die Meldungen mit hoher Relevanz prüfen und umsetzen.

Lageübersicht

ID	Meldung	Relevanz
L-01	**Palo Alto PAN-OS: Lücke in der Management-Oberfläche wird bereits ausgenutzt (CVE-2026-0322, CVSS 4.0: 8,6, 14.10.)**	HOCH
L-02	**Nachtrag Moxa MGate MB3170/MB3270: zwei schwere Lücken in Modbus-Gateways (CVE-2026-86325, CVSS 4.0: 9,4; CVE-2026-86326: 8,6)**	HOCH
L-03	**Cybervorfall beim Baukonsortium des Fehmarnbelt-Tunnels (13.10.)**	HOCH
L-04	**SOCRadar meldet: Initial Access Broker „CyberXero“ soll ukrainische Energieunternehmen ausgespäht und Kundendaten gestohlen haben (Bericht vom 06.10., Medien seit 12.10.)**	HOCH
L-05	**Update SonicWall SMA1000: Angriffe auf die kritische Remote-Access-Lücke (CVE-2026-102255, CVSS 10,0)**	MITTEL
L-06	**Cisco Secure Email Gateway: Zero-Day mit root-Rechten über einen präparierten Mailanhang (CVE-2026-76519, 14.10.)**	MITTEL
L-07	**ENISA, E.DSO, EE-ISAC und ENCS: Europas Energiesektor reagiert zu langsam auf Bedrohungen**	MITTEL
L-08	**Siemens: weitere Advisories vom Patchday, u. a. PSS SINCAL**	MITTEL
L-09	**Qilin führt auf der Leak-Site einen kommunalen Wasserversorger in Mexiko und einen Gasversorger in Nigeria als Opfer (13. und 15.10.)**	MITTEL
L-10	**Booz Allen: KI-Modelle erreichen im OT-Labor alle acht Angriffsziele (13.10.)**	MITTEL
L-11	**Update Eichstätt: Stadt spricht von kopierten Verwaltungsdaten, Ermittler noch vorsichtig (15.10.)**	MITTEL

Meldungen im Detail

L-01 **Palo Alto PAN-OS: Lücke in der Management-Oberfläche wird bereits ausgenutzt (CVE-2026-0322, CVSS 4.0: 8,6, 14.10.)**

Relevanz: **HOCH**

Wer gültige Admin-Zugangsdaten hat und die Management-Oberfläche erreicht, kann Code als root ausführen. Betroffen sind PA-Series, VM-Series und Panorama mit PAN-OS 10.2 bis 12.2. Cloud NGFW und Prisma Access sind nicht betroffen. Palo Alto meldet „very limited exploitation“. Die CISA hat die Lücke am 14.10. in den KEV-Katalog aufgenommen. Für die meisten Versionsstände gibt es bereits Hotfixes (für 11.2 etwa 11.2.4-h22, 11.2.7-h21, 11.2.10-h15 und 11.2.13-h3); nur für 11.2.14 bis 11.2.15 war die Fix-Version 11.2.16 erst für den 15.10. angekündigt. Unsere Einschätzung: Bei Stadtwerken und Produktionsbetrieben schützen PAN-OS-Firewalls oft die Grenze zwischen IT und OT. Deshalb jetzt patchen und die Management-Oberfläche nur aus einem eigenen Admin-Netz bzw. über einen Jump Host erreichbar machen – auf 11.2.14 und 11.2.15 ist das bis zum Fix die wichtigste Übergangsmaßnahme (SANS Critical Control 2, Defensible Architecture).

Quelle: <https://security.paloaltonetworks.com/CVE-2026-0322>

Quelle: <https://www.bleepingcomputer.com/news/security/palo-alto-networks-warns-of-pan-os-rce-flaw-exploited-in-attacks/>

Quelle:

<https://www.cisa.gov/news-events/alerts/2026/10/14/cisa-adds-four-known-exploited-vulnerabilities-catalog>

L-02 **Nachtrag Moxa MGate MB3170/MB3270: zwei schwere Lücken in Modbus-Gateways (CVE-2026-86325, CVSS 4.0: 9,4; CVE-2026-86326: 8,6)**

Relevanz: **HOCH**

Laut CVE-Datenbanken kann ein Konto, das nur lesen darf, in der Kontoverwaltung einen Pufferüberlauf auslösen; damit lassen sich Zugangsdaten auslesen oder ein Denial of Service erzeugen. Dazu kommt eine schwache Prüfung der Firmware-Signatur. Betroffen ist Firmware bis v4.7. Eine Ausnutzung oder ein PoC ist nicht bekannt. Das Advisory von Moxa selbst haben wir nicht gefunden, die Angaben stammen aus CVE-Datenbanken. Unsere Einschätzung: Solche Protocol-Gateways stecken in DACH oft in Wasser- und Abwasseranlagen und Umspannwerken – Firmware-Stand ins Asset-Inventar aufnehmen und Update einplanen (SANS Critical Control 5, Risk-Based Vulnerability Management).

Quelle: <https://app.opencve.io/cve/CVE-2026-86325>

Quelle: <https://securityonline.info/moxa-mgate-vulnerabilities/>

L-03 **Cybervorfall beim Baukonsortium des Fehmarnbelt-Tunnels (13.10.)**

Relevanz: **HOCH**

Femern A/S meldet einen Cybervorfall („cyberhændelse“) bei Femern Link Contractors. Das Konsortium baut den Absenktunnel und die Tunnelelemente. Laut dänischen Medien liegen mehrere Schiffe still, und die Beschäftigten dürfen ihre Rechner nicht nutzen; auch die elektronischen Zugangskarten sollen zeitweise ausgefallen sein. Diese Angaben sind nicht offiziell bestätigt. Art des Vorfalls und Verursacher sind offen. Unsere Einschätzung: Fällt die IT bei einem Auftragnehmer aus, kann das ein Infrastrukturprojekt auch auf der Baustelle ausbremsen – Notfallpläne sollten Auftragnehmer und Baustellen-IT einschließen (SANS Critical Control 1, ICS Incident Response).

Quelle:

<https://femern.com/da/presse/nyheder/hovedentreprenor-pa-femern-projektet-ramt-af-cyberhaendelse/>

Quelle: <https://ing.dk/artikel/fehmarbelt-tunnel-project-hit-cyber-attack>

L-04 **SOCRadar meldet: Initial Access Broker „CyberXero“ soll ukrainische Energieunternehmen ausgespäht und Kundendaten gestohlen haben (Bericht vom 06.10., Medien seit 12.10.)**

Relevanz: **HOCH**

Laut SOCRadar ist „CyberXero“ ein russischsprachiger, finanziell motivierter Initial Access Broker; einen Verkauf von Zugängen konnte SOCRadar selbst nicht nachweisen. Bei vier ukrainischen Organisationen nennt der Bericht den Abfluss von zusammen mehr als 628.000 Datensätzen, davon 564.073 Kundendatensätze eines Fernwärmeversorgers in Charkiw. Sieben Energieunternehmen, darunter der nationale Übertragungsnetzbetreiber, wurden laut SOCRadar nur ausgespäht – ein Einbruch dort ist nicht bestätigt. Für die Angriffe setzte der Akteur laut SOCRadar Claude Code mit bis zu 51 spezialisierten KI-Agenten ein. Behörden wie CERT-UA haben die Angaben bisher nicht bestätigt; alle Medienberichte stützen sich auf SOCRadar. Unsere Einschätzung: Automatisierte Angriffe auf Webseiten, Kundenportale und Remote-Access-Zugänge werden billiger und schneller – auch kleine Versorger in Bayern und Österreich sollten ihre extern erreichbaren Systeme kennen und Schwachstellen nach Risiko patchen (SANS Critical Control 5, Risk-Based Vulnerability Management).

Quelle: <https://socradar.io/blog/cyberxero-ai-iab-ukraine-critical-infrastructure/>

Quelle: <https://thehackernews.com/2026/10/cyberxero-uses-claude-code-in-campaign.html>

Quelle: <https://securityaffairs.com/200803/cyber-crime/cyberxero-used-51-ai-agents-to-steal-628000-ukrainian-records.html>

L-05 **Update SonicWall SMA1000: Angriffe auf die kritische Remote-Access-Lücke (CVE-2026-102255, CVSS 10,0)**

Relevanz: **MITTEL**

Über die Work-Place-Oberfläche ist eine SSRF ohne Anmeldung möglich. Betroffen sind die Modelle SMA 6210, 7210 und 8200v. Der Patch steckt in den Hotfixes 12.4.3-03670 und 12.5.0-03082 und ist seit 06.10. verfügbar. Honeypot-Betreiber verzeichnen Angriffe auf den internen CouchDB-Dienst, heise und BleepingComputer melden die Lücke als ausgenutzt. SonicWall selbst meldet keine aktive Ausnutzung, im KEV-Katalog der CISA steht die Lücke noch nicht. Unsere Einschätzung: Bei Versorgern und Maschinenbauern dienen SMA-Appliances oft der Fernwartung von Anlagen – Patch-Stand jetzt prüfen (SANS Critical Control 4, Secure Remote Access).

Quelle: <https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0017>

Quelle:

<https://www.heise.de/news/Jetzt-patchen-SonicWall-SMA1000-im-Fokus-von-Angreifern-11485407.html>

Quelle: <https://www.bleepingcomputer.com/news/security/max-severity-sonicwall-sma1000-flaw-now-exploited-in-attacks/>

L-06 **Cisco Secure Email Gateway: Zero-Day mit root-Rechten über einen präparierten Mailanhang (CVE-2026-76519, 14.10.)**

Relevanz: MITTEL

Über einen Path Traversal in der AMP-Dateiprüfung lassen sich Befehle als root ausführen, eine Anmeldung ist nicht nötig. Betroffen sind Gateways mit aktivierter File Reputation und Content Scanner Tools älter als 25.3.0.5525. Cisco bestätigt Angriffe und hat IOCs veröffentlicht. Die CISA führt die Lücke seit 14.10. im KEV-Katalog. Unsere Einschätzung: Ein übernommenes Mail-Gateway verschafft Initial Access in die IT – und von dort ist der Weg in schlecht segmentierte OT-Netze kurz.

Quelle:

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-afw-zqYjkjxp>

Quelle: <https://www.bleepingcomputer.com/news/security/cisco-patches-actively-exploited-secure-email-gateway-zero-day/>

L-07 **ENISA, E.DSO, EE-ISAC und ENCS: Europas Energiesektor reagiert zu langsam auf Bedrohungen**

Relevanz: MITTEL

Auf dem 9. Cybersecurity Forum in Brüssel warnten die Fachleute, dass Regulierung allein nicht reicht. Gefahr sehen sie durch geopolitisch motivierte Angriffe, durch KI und durch vernetzte Energietechnik wie Wechselrichter und Edge-Geräte; als Beispiel nannten sie den Angriff auf polnische Wind- und Solarparks im Dezember 2025. Sie empfehlen unabhängige Penetrationstests, Schwachstellenmanagement bei den Herstellern, Informationsaustausch und die Umsetzung von NIS2 und des Network Code on Cybersecurity. Unsere Einschätzung: Für Netzbetreiber und Stadtwerke in DACH ist das eine klare Aufgabenliste für 2027.

Quelle: <https://industrialcyber.co/critical-infrastructure/enisa-e-dso-ee-isac-encs-flag-growing-cyber-risks-to-europes-energy-infrastructure-from-ai-connected-devices/>

L-08 **Siemens: weitere Advisories vom Patchday, u. a. PSS SINCAL**

Relevanz: MITTEL

PSS SINCAL ist eine Software für Netzplanung und Netzberechnung, die bei vielen Stadtwerken und Netzbetreibern läuft. Hoch eingestuft sind laut SecurityWeek außerdem Advisories zu RUGGEDCOM APE1808 und zur .NET Client Library für die S7 Webserver API, mittel eingestuft SENTRON 3NA COM Fuse und Capital Embedded AR Classic. Details und CVEs stammen aus der Übersicht von SecurityWeek, nicht direkt von Siemens ProductCERT. Unsere Einschätzung: Wer PSS SINCAL oder RUGGEDCOM einsetzt, sollte die Advisories bei Siemens ProductCERT nachlesen und das Update einplanen.

Quelle: <https://www.securityweek.com/ics-patch-tuesday-siemens-issues-17-advisories-rockwell-fixes-armorblock-takeover-flaw/>

L-09 **Qilin führt auf der Leak-Site einen kommunalen Wasserversorger in Mexiko und einen Gasversorger in Nigeria als Opfer (13. und 15.10.)**

Relevanz: MITTEL

Unabhängig bestätigt ist keiner der beiden Fälle, einen DACH-Bezug gibt es nicht. Unsere Einschätzung: Qilin greift weiter kommunale Versorger an und ist auch in Deutschland aktiv – ein guter Anlass, bei Stadtwerken Remote Access, Backups und die Segmentierung zwischen IT und OT zu prüfen.

Quelle: <https://ransomware.live/activity/Energy%20%20Utilities>

L-10 **Booz Allen: KI-Modelle erreichen im OT-Labor alle acht Angriffsziele (13.10.)**

Relevanz: MITTEL

In einer isolierten Testanlage mit echten Steuerungen, SCADA und einem Roboterarm kamen ungenannte „Frontier“-Modelle in gut 16 Minuten vom Perimeter bis in die Steuerungsebene, vor allem über Standardprotokolle und Standardpasswörter. Jede physische Aktion musste ein Mensch freigeben. Die Studie belegt keinen echten Angriff. Unsere Einschätzung: Ein gutes Argument für Segmentierung und für den Wechsel von Standardpasswörtern (SANS Critical Control 2, Defensible Architecture).

Quelle: <https://www.helpnetsecurity.com/?p=387525>

Quelle: <https://www.theregister.com/a/5302450>

L-11 **Update Eichstätt: Stadt spricht von kopierten Verwaltungsdaten, Ermittler noch vorsichtig (15.10.)**

Relevanz: MITTEL

Laut Haufe teilte die Stadt mit, dem oder den Tätern sei es gelungen, „sich einen Großteil der Daten der Stadtverwaltung zu kopieren“. Welche Daten genau abgeflossen sind, ist laut Stadt noch unklar; die Ermittler halten noch für offen, ob und welche Daten abgeflossen sind. Die Zentralstelle Cybercrime Bayern geht von Ransomware aus. Die Stadtwerke sind laut Stadt nicht betroffen. Unsere Einschätzung: Solche Vorfälle zeigen, warum Verwaltungsnetze und die Netze kommunaler Versorger getrennt sein sollten (SANS Critical Control 2, Defensible Architecture).

Quelle: https://www.haufe.de/oeffentlicher-dienst/digitalisierung-transformation/cyberangriff-auf-eichstaett_524786_700574.html

Quelle: <https://abendzeitung-muenchen.de/bayern/eichstaett-nach-cyberangriff-erste-dienste-laufen-wieder-art-1165736>

Einordnung und Unterstützung: OT-Cyber.de · Am Esbaum 12, 83022 Rosenheim · +49 8031 8603164 · akademie@ot-cyber.de · <https://ot-cyber.de/>