OT-CYBER.DE

LAGEBILD

OT-/Cyber-Lagebild

Ausgabe 22.10.2026, 16:31 Uhr · Betreiber und Maschinenbauer in Bayern, Salzburg, Tirol und ganz DACH

Zielgruppe	Stadtwerke, Wasser- und Energieversorger, Industrie, Maschinenbau, KRITIS
Datum	22.10.2026
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 7 Meldungen, davon 0 mit hoher Relevanz für Betreiber in DACH.

GESAMTBEWERTUNG

Mittel – keine akute Lage, Meldungen im regulären Schwachstellen-Management bearbeiten.

Lageübersicht

ID	Meldung	Relevanz
L-01	BIND 9: Lücke erlaubt das Einschleusen von Code in den Nameserver (CVE-2026-94300, CVSS 8,1, 22.10.) Betroffen sind BIND 9.11.0 bis 9.18.50, 9.20.0 bis 9.20.29 und 9.21.0 bis 9.21.26, außerdem die Supported Preview Editions 9.11.3-S1 bis 9.18.50-S1 und 9.20.9-S1 bis 9.20.29-S1. Behoben ist die Lücke in 9.20.30, 9.21.27 und 9.20.30-S1. Ausgelöst wird sie über wieder eingespielte GSS-TSIG-signierte UDP-Pakete, ausnutzbar ist sie aus dem Internet. Einen Workaround gibt es nicht, eine aktive Ausnutzung ist den BIND-Entwicklern nicht bekannt. Ob es für den 9.18-Zweig einen Fix gibt, nennt die Meldung nicht. Stadtwerke und Versorger, die eigene DNS-Server mit BIND betreiben (etwa für ein eigenes Glasfasernetz), sollten den Patch zeitnah einplanen (CC5 Risk-Based Vulnerability Management). Quelle: https://www.heise.de/news/BIND-9-Codeschmuggel-Luecke-im-Nameserver-11497068.html	MITTEL
L-02	Versicherer Resilience: Schadensdaten aus dem Sektor Energie und Versorger (21.10.) Grundlage sind Schadensfälle vom 01.01.2023 bis 05.09.2026. Ransomware macht nur 9 % der Fälle aus, aber rund 70 % der Schadenssummen. E-Mail-Kompromittierung steht bei 21 % der Fälle, im übrigen Resilience-Portfolio bei 10 %; Angreifer kamen an MFA vorbei, indem sie Passwörter und Einmalcodes erschlichen oder Sitzungen übernahmen. 17 % der Fälle gingen von Lieferanten und Anbietern aus, im übrigen Portfolio 24 %. In den ausgewerteten Fällen ermöglichten getestete Backups die Wiederherstellung ohne Lösegeld, Segmentierung half einigen Unternehmen, die Produktion zu halten. Resilience schreibt selbst, dass Schadensdaten das OT-Risiko unterschätzen. Die Zahlen stammen aus der Zusammenfassung bei Industrial Cyber, den Original-Report haben wir nicht eingesehen. Quelle: https://industrialcyber.co/reports/resilience-reports-energy-and-utilities-sector-faces-rising-cyber-exposure-from-ransomware-vulnerable-ot-systems/	MITTEL
L-03	Oracle-Patchday Oktober 2026: 1295 Sicherheitspatches (21.10.) Laut heise hat Oracle in der Nacht zum 21.10. insgesamt 1295 Sicherheitspatches veröffentlicht. Als kritisch eingestuft sind unter anderem WebLogic Server, Fusion Middleware, die Datenbank (wegen OpenSSL), MySQL Server, Identity Manager, Access Manager und Managed File Transfer. Bei VirtualBox findet der eingebaute Updater die Version 7.2.22 noch nicht und hält 7.2.20 für aktuell, das Update muss von Hand installiert werden. Für Versorger zählt das aus unserer Sicht vor allem bei Abrechnungs- und ERP-Systemen und bei Middleware an der IT/OT-Grenze. Oracle-Utilities-Produkte nennt die Quelle nicht, das lässt sich in Oracles CPU-Übersicht nachprüfen. Quelle: https://www.heise.de/news/Patchday-bei-Oracle-1295-Sicherheitspatches-quer-durch-die-Bank-11495244.html	MITTEL

ID	Meldung	Relevanz
L-04	UPDATE: Kritische PHP-Lücken (CVE-2026-109618 und CVE-2026-109619): Münster nimmt städtische Webseiten vorsorglich vom Netz (21.10.): Nach Angaben der Stadt hat der kommunale IT-Dienstleister citeq vorsorglich alle externen Verbindungen gekappt. Die städtischen Webseiten sind deshalb nicht erreichbar, die Wiederherstellung dauert mindestens bis Donnerstag, 22.10. Die Universität Münster hat ihre Webdienste seit dem 21.10. nur für Zugriffe aus dem öffentlichen Internet gesperrt, im Uni-Netz und per VPN laufen sie weiter. Clemenshospital, Raphaelsklinik und die Alexianer haben laut ms-aktuell vorsorglich Webservices wie Online-Formulare und Login-Bereiche abgeschaltet. Bislang sind dort keine Daten betroffen, einen bestätigten Angriff gibt es nicht, und die medizinische Versorgung ist nicht eingeschränkt. Laut ms-aktuell sind die vorsorglichen Abschaltungen bislang kein Beleg für einen erfolgreichen Angriff. Zeitweise waren am Mittwochabend auch Internetangebote der Stadtwerke Münster und des Bistums betroffen, ob das mit der PHP-Lücke zusammenhängt, ist offen. Quellen: https://ms-aktuell.de/muenster/php-sicherheitsluecke-in-muenster-stadt und https://www.uni-muenster.de/news/view.php?cmdid=15724 (Erstmeldung am 21.10.2026: https://ot-cyber.de/ot-lage/2026-10-21.html)	MITTEL
L-05	UPDATE: Festo CEPE mit Festo AX OS (Basis PLCnext): OpenSSL-Lücken, Patch noch nicht verfügbar (VDE-2026-090, 20.10.): CVE-2025-15467 (CVSS 9,8) ist ein Out-of-Bounds Write beim Parsen von CMS-Daten und kann bis zur Codeausführung führen. Dazu kommt CVE-2025-69419. Beide betreffen das Verarbeiten von Dateien wie PKCS#12, CMS/PKCS#7 und Schlüsseldateien. Festo empfiehlt AX OS 26.3.1.4, sobald die Version verfügbar ist. Weil das System auf PLCnext aufbaut, sollte man auch Phoenix-Contact-Advisories im Blick behalten. Quelle: https://certvde.com/en/advisories/VDE-2026-090/ (Erstmeldung am 21.10.2026: https://ot-cyber.de/ot-lage/2026-10-21.html)	MITTEL
L-06	Update: Angriff auf die Kühlsteuerungen in Frankreich, der CRA zwingt die Hersteller nicht zu Patches (The Record, 20.10.): Laut ENISA gelten die Pflichten zur Behebung von Schwachstellen nur im Supportzeitraum. Die angegriffenen Danfoss AK-SM/AK-SC (End-of-Life 2016 bzw. 2021) und die xweb-Geräte von Copeland und Dixell fallen deshalb nicht darunter. Die Meldepflicht für ausgenutzte Lücken gilt aber auch für Altgeräte. Die Pariser Staatsanwaltschaft schätzt rund 700 Opfer, die ANSSI rät, exponierte Controller vom Netz zu nehmen oder zu filtern. Für Versorger heißt das: Bei End-of-Life-Steuerungen hilft kein Hersteller-Patch, dann schützen vor allem Segmentierung, ein sauberes Asset-Inventar und Steuerungen, die nicht offen im Internet stehen. Quelle: https://therecord.media/eu-cyber-law-wont-force-fixes-for-fridges-in-french-attack	MITTEL
L-07	NCC Group: Ransomware im 3. Quartal 2026 um 23 % gestiegen, Industrie am stärksten betroffen (21.10.): Auf die Industrie entfielen 838 Angriffe. Die aktivsten Gruppen waren Qilin (365) und The Gentlemen (359), in Europa zählte NCC allein im September 211 Angriffe. Eine eigene Zahl für Versorger oder Energie gibt es nicht. Den NCC-Bericht selbst habe ich nicht gefunden, die Zahlen stammen nur aus der Presse. Quelle: https://securityt oday.com/articles/2026/10/21/industrial-sector-drives-ransomware-surge-in -third-quarter.aspx	MITTEL

Meldungen im Detail

L-01 BIND 9: Lücke erlaubt das Einschleusen von Code in den Nameserver (CVE-2026-94300, CVSS 8,1, 22.10.) Betroffen sind BIND 9.11.0 bis 9.18.50, 9.20.0 bis 9.20.29 und 9.21.0 bis 9.21.26, außerdem die Supported Preview Editions 9.11.3-S1 bis 9.18.50-S1 und 9.20.9-S1 bis 9.20.29-S1. Behoben ist die Lücke in 9.20.30, 9.21.27 und 9.20.30-S1. Ausgelöst wird sie über wieder eingespielte GSS-TSIG-signierte UDP-Pakete, ausnutzbar ist sie aus dem Internet. Einen Workaround gibt es nicht, eine aktive Ausnutzung ist den BIND-Entwicklern nicht bekannt. Ob es für den 9.18-Zweig einen Fix gibt, nennt die Meldung nicht. Stadtwerke und Versorger, die eigene DNS-Server mit BIND betreiben (etwa für ein eigenes Glasfasernetz), sollten den Patch zeitnah einplanen (CC5 Risk-Based Vulnerability Management). Quelle: https://www.heise.de/news/BIND-9-Codeschmuggel-Luecke-im-Nameserver-11497068.html

Relevanz: MITTEL

L-02 Versicherer Resilience: Schadensdaten aus dem Sektor Energie und Versorger (21.10.) Grundlage sind Schadensfälle vom 01.01.2023 bis 05.09.2026. Ransomware macht nur 9 % der Fälle aus, aber rund 70 % der Schadenssummen. E-Mail-Kompromittierung steht bei 21 % der Fälle, im übrigen Resilience-Portfolio bei 10 %; Angreifer kamen an MFA vorbei, indem sie Passwörter und Einmalcodes erschlichen oder Sitzungen übernahmen. 17 % der Fälle gingen von Lieferanten und Anbietern aus, im übrigen Portfolio 24 %. In den ausgewerteten Fällen ermöglichten getestete Backups die Wiederherstellung ohne Lösegeld, Segmentierung half einigen Unternehmen, die Produktion zu halten. Resilience schreibt selbst, dass Schadensdaten das OT-Risiko unterschätzen. Die Zahlen stammen aus der Zusammenfassung bei Industrial Cyber, den Original-Report haben wir nicht eingesehen. Quelle: https://industrialcyber.co/reports/resilience-reports-energy-and-utilities-sector-faces-rising-cyber-exposure-from-ransomware-vulnerable-ot-systems/

Relevanz: MITTEL

L-03 Oracle-Patchday Oktober 2026: 1295 Sicherheitspatches (21.10.) Laut heise hat Oracle in der Nacht zum 21.10. insgesamt 1295 Sicherheitspatches veröffentlicht. Als kritisch eingestuft sind unter anderem WebLogic Server, Fusion Middleware, die Datenbank (wegen OpenSSL), MySQL Server, Identity Manager, Access Manager und Managed File Transfer. Bei VirtualBox findet der eingebaute Updater die Version 7.2.22 noch nicht und hält 7.2.20 für aktuell, das Update muss von Hand installiert werden. Für Versorger zählt das aus unserer Sicht vor allem bei Abrechnungs- und ERP-Systemen und bei Middleware an der IT/OT-Grenze. Oracle-Utilities-Produkte nennt die Quelle nicht, das lässt sich in Oracles CPU-Übersicht nachprüfen. Quelle: https://www.heise.de/news/Patchday-bei-Oracle-1295-Sicherheitspatches-quer-durch-die-Bank-11495244.html

Relevanz: MITTEL

L-04 🔄 UPDATE: Kritische PHP-Lücken (CVE-2026-109618 und CVE-2026-109619): Münster nimmt städtische Webseiten vorsorglich vom Netz (21.10.): Nach Angaben der Stadt hat der kommunale IT-Dienstleister citeq vorsorglich alle externen Verbindungen gekappt. Die städtischen Webseiten sind deshalb nicht erreichbar, die Wiederherstellung dauert mindestens bis Donnerstag, 22.10. Die Universität Münster hat ihre Webdienste seit dem 21.10. nur für Zugriffe aus dem öffentlichen Internet gesperrt, im Uni-Netz und per VPN laufen sie weiter. Clemenshospital, Raphaelsklinik und die Alexianer haben laut ms-aktuell vorsorglich Webservices wie Online-Formulare und Login-Bereiche abgeschaltet. Bislang sind dort keine Daten betroffen, einen bestätigten Angriff gibt es nicht, und die medizinische Versorgung ist nicht eingeschränkt. Laut ms-aktuell sind die vorsorglichen Abschaltungen bislang kein Beleg für einen erfolgreichen Angriff. Zeitweise waren am Mittwochabend auch Internetangebote der Stadtwerke Münster und des Bistums betroffen, ob das mit der PHP-Lücke zusammenhängt, ist offen. Quellen: https://ms-aktuell.de/muenster/php-sicherheitsluecke-in-muenster-stadt und https://www.uni-muenster.de/news/view.php?cmdid=15724 (Erstmeldung am 21.10.2026: https://ot-cyber.de/ot-lage/2026-10-21.html)

Relevanz: MITTEL

L-05 🔄 UPDATE: Festo CEPE mit Festo AX OS (Basis PLCnext): OpenSSL-Lücken, Patch noch nicht verfügbar (VDE-2026-090, 20.10.): CVE-2025-15467 (CVSS 9,8) ist ein Out-of-Bounds Write beim Parsen von CMS-Daten und kann bis zur Codeausführung führen. Dazu kommt CVE-2025-69419. Beide betreffen das Verarbeiten von Dateien wie PKCS#12, CMS/PKCS#7 und Schlüsseldateien. Festo empfiehlt AX OS 26.3.1.4, sobald die Version verfügbar ist. Weil das System auf PLCnext aufbaut, sollte man auch Phoenix-Contact-Advisories im Blick behalten. Quelle: https://certvde.com/en/advisories/VDE-2026-090/ (Erstmeldung am 21.10.2026: https://ot-cyber.de/ot-lage/2026-10-21.html)

Relevanz: MITTEL

L-06 Update: Angriff auf die Kühlsteuerungen in Frankreich, der CRA zwingt die Hersteller nicht zu Patches (The Record, 20.10.): Laut ENISA gelten die Pflichten zur Behebung von Schwachstellen nur im Supportzeitraum. Die angegriffenen Danfoss AK-SM/AK-SC (End-of-Life 2016 bzw. 2021) und die xweb-Geräte von Copeland und Dixell fallen deshalb nicht darunter. Die Meldepflicht für ausgenutzte Lücken gilt aber auch für Altgeräte. Die Pariser Staatsanwaltschaft schätzt rund 700 Opfer, die ANSSI rät, exponierte Controller vom Netz zu nehmen oder zu filtern. Für Versorger heißt das: Bei End-of-Life-Steuerungen hilft kein Hersteller-Patch, dann schützen vor allem Segmentierung, ein sauberes Asset-Inventar und Steuerungen, die nicht offen im Internet stehen. Quelle: https://therecord.media/eu-cyber-law-wont-force-fixes-for-fridges-in-french-attack

Relevanz: MITTEL

L-07 NCC Group: Ransomware im 3. Quartal 2026 um 23 % gestiegen, Industrie am stärksten betroffen (21.10.): Auf die Industrie entfielen 838 Angriffe. Die aktivsten Gruppen waren Qilin (365) und The Gentlemen (359), in Europa zählte NCC allein im September 211 Angriffe. Eine eigene Zahl für Versorger oder Energie gibt es nicht. Den NCC-Bericht selbst habe ich nicht gefunden, die Zahlen stammen nur aus der Presse. Quelle: https://securitytoday.com/articles/2026/10/21/industrial-sector-drives-ransomware-surge-in-third-quarter.aspx

Relevanz: MITTEL

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