OT-CYBER.DE

LAGEBILD

OT-/Cyber-Lagebild

Ausgabe 02.11.2026, 16:09 Uhr · Betreiber und Maschinenbauer in Bayern, Salzburg, Tirol und ganz DACH

Zielgruppe	Stadtwerke, Wasser- und Energieversorger, Industrie, Maschinenbau, KRITIS
Datum	02.11.2026
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 5 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	Synology warnt: Ransomware greift NAS mit veralteter DSM-Software an (Herstellermeldung vom 29.10.): Laut Synology nutzen Angreifer eine Schwachstelle aus, die schon im Dezember 2024 geschlossen wurde, um Geräte mit veraltetem DiskStation Manager (DSM) zu verschlüsseln und Lösegeld zu erpressen. Eine CVE nennt der Hersteller nicht, er verweist auf sein Advisory Synology-SA-24:20 und rät, DSM sofort zu aktualisieren und automatische Updates einzuschalten. Meine Einschätzung (Max Gilg): Synology-NAS können bei Stadtwerken und Maschinenbauern als Backup- oder Projektablage neben der Leittechnik stehen. Wer dort Sicherungen der Anlagen ablegt, sollte DSM aktualisieren, die Verwaltungsoberfläche nicht aus dem Internet erreichbar machen und eine Offline-Kopie der Backups vorhalten (CC1 ICS Incident Response). Quelle: https://www.synology.com/en-global/company/news/article/C3RB3R · https://www.heise.de/news/Schwachstellen-in-Drupal-Ivanti-Connect-Secure-und-Synology-angegriffen-11507497.html	MITTEL
L-02	Progress WS_FTP Server: kritische Lücken, die schwerste mit CVSS 10,0 (CVE-2026-84295): Laut heise können nicht angemeldete Angreifer bei WS_FTP Server unter Windows über eine unzureichende Authentifizierung sensible Informationen abgreifen, auch Admin-Zugangsdaten. Diese Lücke ist ab Version 2024.0.6 bzw. 2025.0.3 behoben. Die meisten weiteren Lücken, darunter OS Command Injection und Path Traversal, schließen erst die Versionen 2024.0.7 bzw. 2025.0.4, die seit dem 1. Oktober bereitstehen. Eine Ausnutzung meldet heise bisher nicht. Meine Einschätzung (Max Gilg): Dateitransfer-Server für den Austausch mit Dienstleistern, etwa für Mess- oder Abrechnungsdaten, gehören ins Asset-Inventar und auf die aktuelle Version (CC5 Risk-Based Vulnerability Management). Quelle: https://www.heise.de/news/Sicherheitsluecken-in-Progress-WS-FTP-ermoeglichen-Kompromittierung-11507580.html	MITTEL

ID	Meldung	Relevanz
L-03	Gefälschte Warnungen über die Warn-Apps in der Ukraine und in Russland (Nacht vom 1. auf den 2.11.): Am späten Abend des 1.11. hat die ukrainische App „Air Alert“ falsche Warnungen verschickt, unter anderem vor radioaktiver Strahlung in Kiew, laut Kyiv Independent auch vor einem Chemieangriff. Die ukrainische Luftwaffe schrieb auf Telegram, die App sei wahrscheinlich „vom Feind kompromittiert“ worden, eine Strahlengefahr bestehe nicht. Laut Kyiv Independent meldete die App gegen 2 Uhr Ortszeit, der Betrieb werde schrittweise wiederhergestellt. In der Nacht zum 2.11. meldete die russische Staatsagentur TASS unter Berufung auf das Zivilschutzministerium einen „massiven Cyberangriff“ auf dessen Warn-App, über die laut Ministerium Falschinformationen verschickt wurden. Das landesweite Warnsystem selbst funktioniere laut Ministerium normal. Das Ministerium nannte keine Verdächtigen. Meine Einschätzung (Max Gilg): Wer Alarmierungswege kapert, löst Panik aus, ohne eine Industrieanlage anzufassen. Stadtwerke und Wasserversorger in DACH sollten ihre Kanäle für Störungs- und Bürgerinformation (App, SMS-Dienst, Webseite, Social Media) in die Notfallplanung aufnehmen und festlegen, wie sie eine Falschmeldung schnell widerrufen (CC1 ICS Incident Response). Quellen: https://www.heise.de/news/Apps-fuer-Notfall-Warnungen-in-Ukraine-und-Russland-geknackt-11507440.html · https://kyivindependent.com/ukraines-air-raid-alert-system-hacked-air-force-says-as-false-nuclear-chemical-warnings-sound/	MITTEL
L-04	Datensicherheitsvorfall beim Betreiber des Kernkraftwerks South Texas Project (Bericht vom 30.10.): Die STP Nuclear Operating Co. hat der Generalstaatsanwaltschaft von Texas einen „data security incident“ gemeldet. Betroffen sind knapp 1.200 Menschen in Texas, offengelegt wurden Namen, Sozialversicherungsnummern, Geburtsdaten und weitere persönliche Angaben. Die Betroffenen wurden per E-Mail informiert. Die Ursache ist offen, eine Auswirkung auf Betriebs- oder Sicherheitssysteme ist nicht bekannt. Die Aufsichtsbehörde NRC sieht die Anlage weiter „operating safely and securely“. Meine Einschätzung (Max Gilg): Auch bei Betreibern in DACH sollte die Meldung eines IT-Vorfalls klar sagen, ob die Leittechnik betroffen war. Wer das nicht belegen kann, braucht eine saubere Trennung von IT und OT und eine Angriffserkennung im OT-Netz (CC2 Defensible Architecture, CC3 ICS Network Visibility & Monitoring). Quelle: https://www.govtech.com/security/data-breach-hits-operator-of-south-texas-nuclear-power-plant	MITTEL
L-05	Nozomi Networks beschreibt das neue DDoS-Botnetz „Kairos“ (Blog „Kairos Hold'em“ vom 29.10.): Der Bot ist in Go geschrieben, läuft unter Linux und macht kompromittierte Geräte zu Angriffsknoten, die hunderte bis tausende TCP-Verbindungen zum Ziel offen halten. Den Zugang bekamen die Angreifer ohne Exploit: über Telnet mit dem Benutzer „root“ und leerem Passwort, beobachtet auf Honeypots von Nozomi. Neben x86_64 fand Nozomi per VirusTotal-Suche Varianten für ARM, MIPS und 32-Bit-x86, der Loader weicht auf BusyBox aus und läuft so auch auf schlanken Embedded-Systemen. Nozomi veröffentlicht IoCs (C2- und Download-Adressen, SHA-256-Hashes), eine YARA-Regel und eine Netzwerk-Regel („Packet Rule“, Syntax wie Snort/Suricata), die die Anmeldung „REGISTER linux“ auf TCP-Port 9999 erkennt. Meine Einschätzung (Max Gilg): Ein offener Telnet-Zugang mit leerem Root-Passwort findet sich in Anlagennetzen immer noch auf Gateways, Kameras und alten Embedded-Geräten. Telnet abschalten, Standardpasswörter ersetzen und den Netzverkehr auf ungewöhnliche Verbindungen nach außen überwachen (CC3 ICS Network Visibility & Monitoring). Quelle: https://www.nozominetworks.com/blog/kairos-holdem-dissecting-a-new-go-based-ddos-botnet	MITTEL

Meldungen im Detail

L-01 Synology warnt: Ransomware greift NAS mit veralteter DSM-Software an (Herstellermeldung vom 29.10.): Laut Synology nutzen Angreifer eine Schwachstelle aus, die schon im Dezember 2024 geschlossen wurde, um Geräte mit veraltetem DiskStation Manager (DSM) zu verschlüsseln und Lösegeld zu erpressen. Eine CVE nennt der Hersteller nicht, er verweist auf sein Advisory Synology-SA-24:20 und rät, DSM sofort zu aktualisieren und automatische Updates einzuschalten. Meine Einschätzung (Max Gilg): Synology-NAS können bei Stadtwerken und Maschinenbauern als Backup- oder Projektablage neben der Leittechnik stehen. Wer dort Sicherungen der Anlagen ablegt, sollte DSM aktualisieren, die Verwaltungsoberfläche nicht aus dem Internet erreichbar machen und eine Offline-Kopie der Backups vorhalten (CC1 ICS Incident Response). Quelle: https://www.synology.com/en-global/company/news/article/C3RB3R · https://www.heise.de/news/Schwachstellen-in-Drupal-Ivanti-Connect-Secure-und-Synology-angegriffen-11507497.html

Relevanz: MITTEL

L-02 Progress WS_FTP Server: kritische Lücken, die schwerste mit CVSS 10,0 (CVE-2026-84295): Laut heise können nicht angemeldete Angreifer bei WS_FTP Server unter Windows über eine unzureichende Authentifizierung sensible Informationen abgreifen, auch Admin-Zugangsdaten. Diese Lücke ist ab Version 2024.0.6 bzw. 2025.0.3 behoben. Die meisten weiteren Lücken, darunter OS Command Injection und Path Traversal, schließen erst die Versionen 2024.0.7 bzw. 2025.0.4, die seit dem 1. Oktober bereitstehen. Eine Ausnutzung meldet heise bisher nicht. Meine Einschätzung (Max Gilg): Dateitransfer-Server für den Austausch mit Dienstleistern, etwa für Mess- oder Abrechnungsdaten, gehören ins Asset-Inventar und auf die aktuelle Version (CC5 Risk-Based Vulnerability Management). Quelle: https://www.heise.de/news/Sicherheitsluecken-in-Progress-WS-FTP-ermoeglichen-Kompromittierung-11507580.html

Relevanz: MITTEL

L-03 Gefälschte Warnungen über die Warn-Apps in der Ukraine und in Russland (Nacht vom 1. auf den 2.11.): Am späten Abend des 1.11. hat die ukrainische App „Air Alert“ falsche Warnungen verschickt, unter anderem vor radioaktiver Strahlung in Kiew, laut Kyiv Independent auch vor einem Chemieangriff. Die ukrainische Luftwaffe schrieb auf Telegram, die App sei wahrscheinlich „vom Feind kompromittiert“ worden, eine Strahlengefahr bestehe nicht. Laut Kyiv Independent meldete die App gegen 2 Uhr Ortszeit, der Betrieb werde schrittweise wiederhergestellt. In der Nacht zum 2.11. meldete die russische Staatsagentur TASS unter Berufung auf das Zivilschutzministerium einen „massiven Cyberangriff“ auf dessen Warn-App, über die laut Ministerium Falschinformationen verschickt wurden. Das landesweite Warnsystem selbst funktioniere laut Ministerium normal. Das Ministerium nannte keine Verdächtigen. Meine Einschätzung (Max Gilg): Wer Alarmierungswege kapert, löst Panik aus, ohne eine Industrieanlage anzufassen. Stadtwerke und Wasserversorger in DACH sollten ihre Kanäle für Störungs- und Bürgerinformation (App, SMS-Dienst, Webseite, Social Media) in die Notfallplanung aufnehmen und festlegen, wie sie eine Falschmeldung schnell widerrufen (CC1 ICS Incident Response). Quellen: https://www.heise.de/news/Apps-fuer-Notfall-Warnungen-in-Ukraine-und-Russland-geknackt-11507440.html · https://kyivindependent.com/ukraines-air-raid-alert-system-hacked-air-force-says-as-false-nuclear-chemical-warnings-sound/

Relevanz: MITTEL

L-04 Datensicherheitsvorfall beim Betreiber des Kernkraftwerks South Texas Project (Bericht vom 30.10.): Die STP Nuclear Operating Co. hat der Generalstaatsanwaltschaft von Texas einen „data security incident“ gemeldet. Betroffen sind knapp 1.200 Menschen in Texas, offengelegt wurden Namen, Sozialversicherungsnummern, Geburtsdaten und weitere persönliche Angaben. Die Betroffenen wurden per E-Mail informiert. Die Ursache ist offen, eine Auswirkung auf Betriebs- oder Sicherheitssysteme ist nicht bekannt. Die Aufsichtsbehörde NRC sieht die Anlage weiter „operating safely and securely“. Meine Einschätzung (Max Gilg): Auch bei Betreibern in DACH sollte die Meldung eines IT-Vorfalls klar sagen, ob die Leittechnik betroffen war. Wer das nicht belegen kann, braucht eine saubere Trennung von IT und OT und eine Angriffserkennung im OT-Netz (CC2 Defensible Architecture, CC3 ICS Network Visibility & Monitoring). Quelle: https://www.govtech.com/security/data-breach-hits-operator-of-south-texas-nuclear-power-plant

Relevanz: MITTEL

L-05 Nozomi Networks beschreibt das neue DDoS-Botnetz „Kairos“ (Blog „Kairos Hold'em“ vom 29.10.): Der Bot ist in Go geschrieben, läuft unter Linux und macht kompromittierte Geräte zu Angriffsknoten, die hunderte bis tausende TCP-Verbindungen zum Ziel offen halten. Den Zugang bekamen die Angreifer ohne Exploit: über Telnet mit dem Benutzer „root“ und leerem Passwort, beobachtet auf Honeypots von Nozomi. Neben x86_64 fand Nozomi per VirusTotal-Suche Varianten für ARM, MIPS und 32-Bit-x86, der Loader weicht auf BusyBox aus und läuft so auch auf schlanken Embedded-Systemen. Nozomi veröffentlicht IoCs (C2- und Download-Adressen, SHA-256-Hashes), eine YARA-Regel und eine Netzwerk-Regel („Packet Rule“, Syntax wie Snort/Suricata), die die Anmeldung „REGISTER linux“ auf TCP-Port 9999 erkennt. Meine Einschätzung (Max Gilg): Ein offener Telnet-Zugang mit leerem Root-Passwort findet sich in Anlagennetzen immer noch auf Gateways, Kameras und alten Embedded-Geräten. Telnet abschalten, Standardpasswörter ersetzen und den Netzverkehr auf ungewöhnliche Verbindungen nach außen überwachen (CC3 ICS Network Visibility & Monitoring). Quelle: https://www.nozominetworks.com/blog/kairos-hold em-dissecting-a-new-go-based-ddos-botnet

Relevanz: MITTEL

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