OT-CYBER.DE

LAGEBILD

OT-/Cyber-Lagebild

Ausgabe 20.10.2026, 17:41 Uhr · Betreiber und Maschinenbauer in Bayern, Salzburg, Tirol und ganz DACH

Zielgruppe	Stadtwerke, Wasser- und Energieversorger, Industrie, Maschinenbau, KRITIS
Datum	20.10.2026
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 2 mit hoher Relevanz für Betreiber in DACH.

• **Siemens Software Center: Lücke wird über ClickFix-Köder ausgenutzt (CVE-2026-110936, CVSS 4.0: 8,4, SSA-580366)**

• **Ransomware-Gruppe Settra listet deutschen Anlagenbauer aus der Abwassertechnik (unbestätigt)** Seit spätestens 18.10. ist ein deutscher Anlagenbauer aus der Abwassertechnik auf der Leak-Site der Ransomware-Gruppe „Settra“ gelistet. An diesem Tag hat ransomware.live den Eintrag erfasst. Die Täter behaupten, 140 GB Daten erbeutet zu haben. Den Angriff schätzt ransomware.live auf etwa den 25.09. **Unbestätigt, nur laut Täterangabe:** Eine Stellungnahme der Firma, einer Behörde oder einen Medienbericht haben wir bis zum 20.10. nicht gefunden. Deshalb nennen wir den Namen nicht und verlinken den Leak-Eintrag nicht. Einschätzung: Typischerweise können bei Anlagenbauern für Kläranlagen Projekt- und Automatisierungsunterlagen, Zugänge für die Fernwartung und Kundenlisten von Betreibern liegen. Ob solche Daten hier betroffen sind, ist nicht bekannt. Betreiber, die mit Anlagenbauern aus diesem Bereich arbeiten, sollten prüfen, welche Fernwartungszugänge der Dienstleister hat, und diese bei Bedarf neu vergeben (CC4 Secure Remote Access). Quellen: https://www.ransomware.live/group/settra

GESAMTBEWERTUNG

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

Lageübersicht

ID	Meldung	Relevanz
L-01	**Siemens Software Center: Lücke wird über ClickFix-Köder ausgenutzt (CVE-2026-110936, CVSS 4.0: 8,4, SSA-580366)**	HOCH
L-02	**Supply-Chain-Angriff über manipulierte Update-Konfiguration bei AOMEI Backupper (19.10.)**	MITTEL
L-03	**Update: ConnectWise setzt drei Cloud-Dienste aus (19.10.)**	MITTEL
L-04	**Rheinland-Pfalz: Energieversorgung rückt bei Bedrohungen stärker in den Fokus (19.10.)**	MITTEL
L-05	**Ransomware-Gruppe Settra listet deutschen Anlagenbauer aus der Abwassertechnik (unbestätigt)** Seit spätestens 18.10. ist ein deutscher Anlagenbauer aus der Abwassertechnik auf der Leak-Site der Ransomware-Gruppe „Settra“ gelistet. An diesem Tag hat ransomware.live den Eintrag erfasst. Die Täter behaupten, 140 GB Daten erbeutet zu haben. Den Angriff schätzt ransomware.live auf etwa den 25.09. **Unbestätigt, nur laut Täterangabe:** Eine Stellungnahme der Firma, einer Behörde oder einen Medienbericht haben wir bis zum 20.10. nicht gefunden. Deshalb nennen wir den Namen nicht und verlinken den Leak-Eintrag nicht. Einschätzung: Typischerweise können bei Anlagenbauern für Kläranlagen Projekt- und Automatisierungsunterlagen, Zugänge für die Fernwartung und Kundenlisten von Betreibern liegen. Ob solche Daten hier betroffen sind, ist nicht bekannt. Betreiber, die mit Anlagenbauern aus diesem Bereich arbeiten, sollten prüfen, welche Fernwartungszugänge der Dienstleister hat, und diese bei Bedarf neu vergeben (CC4 Secure Remote Access). Quellen: https://www.ransomware.live/group/settra	HOCH

ID	Meldung	Relevanz
L-06	UPDATE: **Update: Loxone bestätigt kopierte CRM-Daten, Erpresserschreiben nennt 201,6 GB (19.10.)** Laut heise (19.10.) hat Loxone bestätigt, dass Daten kopiert wurden, vor allem aus dem CRM-System (Kontaktdaten von Partnerbetrieben, Supportanfragen) und aus dem Bewerbermanagement. Zu der Datenmenge äußert sich Loxone nicht. Miniserver, Remote Connect und Exosphere sind laut Loxone nicht betroffen, Benutzer- und Zugangsdaten liegen nach Angaben des Herstellers nur lokal am Miniserver. Unbestätigt ist das Erpresserschreiben, das Borns IT-Blog zeigt: Die Angreifer behaupten, 201,6 GB kopiert und verschlüsselt zu haben, und drohen mit Veröffentlichung in etwa drei Tagen (Stand 19.10.). Im Zusammenhang mit veröffentlichten Beispieldaten weist Loxone darauf hin, dass loxwiki nicht von Loxone betrieben wird und nicht auf einer Loxone-Domain läuft. Dass die Ticketing-Plattform teilweise betroffen sei, steht nur in einem Leserkommentar bei Born mit Verweis auf das Loxforum; Loxone selbst nennt kopierte Supportanfragen. Vorsorgliche Empfehlung von uns, nicht von Loxone: Wer Zugangsdaten, API-Zugänge oder Konfigurationen in Supportanfragen an Loxone geschickt hat, sollte diese erneuern. Quellen: https://www.heise.de/news/Loxone-Cyberangriff-auf-Gebaeudeautomatisierungsanbieter-11492872.html , https://borncity.com/blog/2026/10/19/sicherheitsvorfall-bei-loxone/ (Erstmeldung am 19.10.2026: https://ot-cyber.de/ot-lage/2026-10-19.html)	MITTEL
L-07	**Claroty Team82: KI-Agent baut root-Exploit für Danfoss AK-SM 800A in rund 28 Minuten nach** Claroty Team82 hat am 13.10. gezeigt, wie Claude Sonnet 4.6 (mittlerer Reasoning-Modus, im Editor Cursor) bekannte Lücken in der Kühlstellensteuerung Danfoss AK-SM 800A nachbaut. Eigene Forschungsergebnisse von Team82 bekam die KI nicht. Als Eingaben dienten öffentliche CVE-Angaben und Schwachstellenklassen, die frei herunterladbare Firmware und Analysewerkzeuge. Der Agent verkettete zwei der Lücken zur Ausführung von Befehlen als root auf einem Laborgerät. Von der ersten Analyse bis zum funktionierenden Exploit vergingen etwa 28 Minuten, die KI-Nutzung kostete rund 6 US-Dollar. Ganz ohne Menschen ging es nicht: Am Authentication Bypass scheiterte der Agent zunächst. Forscher lenkten die Analyse um und stellten eine Ghidra-Anbindung für das 67 MB große Hauptprogramm bereit. Im früheren Bericht vom 09.08. nennt Claroty 2.765 aus dem Internet erreichbare Geräte laut Censys und die von Danfoss veröffentlichte Firmware R4.3.1. Laut NeoTeo behebt diese Version nach Angaben von Claroty die bekannten Lücken. Unsere Einschätzung: Wenn, wie im Laborversuch, zu einer bekannten Lücke in einer halben Stunde ein Exploit steht, zählt bei OT-Geräten im Internet jeder Tag ohne Patch. Steuerungen gehören nicht direkt ins Internet (CC5 Risk-Based Vulnerability Management). Es ist ein Laborversuch und kein neuer Vorfall. Ob dieser Angriffsweg bei Vorfällen in französischen Supermärkten genutzt wurde, ist laut Claroty nicht bestätigt. Quellen: https://claroty.com/team82/research/firmware-to-root-in-30-minutes-how-ai-is-changing-threat-intelligence , https://claroty.com/team82/research/freeze-the-controller-defrost-the-food-uncovering-vulnerabilities-in-danfoss-refrigeration-controllers , https://www.neoteo.com/en/claroty-says-claude-reproduced-danfoss-flaws-in-about-28-minutes , https://industrialcyber.co/ai/claroty-team82-shows-ai-can-rebuild-danfoss-controller-exploits-in	MITTEL

Meldungen im Detail

L-01 **Siemens Software Center: Lücke wird über ClickFix-Köder ausgenutzt (CVE-2026-110936, CVSS 4.0: 8,4, SSA-580366)**

Relevanz: HOCH

Siemens hat am 19.10. in einem Blogbeitrag von Siemens ProductCERT bestätigt, dass die DLL-Side-Loading-Lücke aktiv ausgenutzt wird. Die Angreifer nutzen eine echte, signierte, verwundbare Version des Software Center (damals 3.5.8.7), die Hilfsdateien aus dem eigenen Ordner ungeprüft lädt, und legen eigene DLLs daneben. Das Malware-Paket „AllMyBasic.msi“ wurde außerhalb der offiziellen Kanäle verteilt; den Verteilweg (2.27.248[.]127) führt Siemens inzwischen als inaktiv. Rechner, die vorher von dort geladen haben, können trotzdem infiziert sein. Siemens ordnet das der Romulus-ClickFix-Kampagne zu. Laut Forescout Vedere Labs (zitiert von Help Net Security) ist eine der Nutzlasten LegionLoader. Systeme, Produkte oder Update-Kanäle von Siemens sind nach Kenntnis des Herstellers nicht kompromittiert. Betroffen sind laut Advisory alle Versionen vor 4.0.9.8; diese Version schließt die Lücke, bestehende Installationen aktualisieren sich beim nächsten Start selbst. Siemens rät, die im Blogbeitrag genannten IoCs zu blockieren (u. a. 96.62.218[.]59 und wizardexpensive[.]com) und nach fremden DLLs neben der Programmdatei zu suchen. Unsere Einschätzung für Stadtwerke und Wasserversorger: Die Angreifer bringen die signierte Kopie selbst mit. Gefährdet ist also jeder Büro- oder Engineering-PC, auf dem der ClickFix-Köder ausgeführt wird, auch ohne installiertes Software Center. Ein Warnzeichen ist das Software Center auf einem PC, auf dem es nie installiert wurde. Bestehende Installationen auf 4.0.9.8 bringen und alle PCs, besonders Engineering-PCs und Jump Hosts an der Schnittstelle zur Leittechnik, auf die IoCs prüfen (CC5 Risk-Based Vulnerability Management). Das Advisory ist vom 15.10., am 17.10. kam die Behebung dazu, am 19.10. der Verweis auf den Blogbeitrag.

Quelle: https://productcert.siemens.com/news/2026/10/19/active-exploitation-of-cve-2026-110936-in-siemens-software-center/

Quelle: https://productcert.siemens.com/productcert/html/ssa-580366.html

Quelle: https://www.helpnetsecurity.com/2026/10/20/exploitation-siemens-software-center-vulnerability-cve-2026-110936/

L-02 **Supply-Chain-Angriff über manipulierte Update-Konfiguration bei AOMEI Backupper (19.10.)**

Relevanz: MITTEL

Laut ManageEngine (Threat Analysis Lab) und Google Threat Intelligence Group/Mandiant hat die Gruppe UNC7017 auf der Infrastruktur von AOMEI zwei Konfigurationsdateien manipuliert (down_html.ini und Notifycfg.ini), nicht die Update-Pakete selbst. In drei kurzen Zeitfenstern (28.05., 16.07. und 20.07.) bekamen Kunden so den bisher unbekannten Downloader CROSSROAD und die Backdoor SHINYROAD, die das legitime Fernwartungswerkzeug Radmin missbraucht. Betroffen waren unter anderem Organisationen in der Schweiz. Die Korrektur auf Serverseite stoppt neue Infektionen, entfernt aber keine Backdoors, die schon installiert wurden. Wer AOMEI Backupper einsetzt, sollte deshalb jetzt nach den veröffentlichten IoCs suchen. Unsere Einschätzung: Backup-Werkzeuge wie dieses kommen auch auf Engineering-Rechnern und Servern in kleineren Betrieben vor.

Quelle: https://www.bleepingcomputer.com/news/security/hackers-hijack-aomei-update-servers-to-secretly-spread-malware/

L-03 **Update: ConnectWise setzt drei Cloud-Dienste aus (19.10.)**

Relevanz: MITTEL

Neben Cloud Backup sind jetzt auch die Plattformen SaaS Security und Cloud Management ausgesetzt. Einen Termin für die Wiederaufnahme gibt es laut ConnectWise nicht. Laut Microsoft haben die Angreifer wahrscheinlich Berechtigungen missbraucht, die der Anwendung erteilt waren, darunter Directory.ReadWrite.All. Huntress warnt, dass sich eine solche Anwendung selbst zum Global Admin machen kann, und hat das in einem Mandanten gesehen. Das Wechseln der Zugangsdaten reicht deshalb nicht. Versorger und IT-Dienstleister mit ConnectWise-Diensten sollten in ihren Microsoft-365-Mandanten Rollen, Anwendungen, deren Berechtigungen und Anmeldemethoden prüfen.

Quelle: https://therecord.media/connectwise-suspends-cloud-backup-service-supply-chain-attack

L-04 **Rheinland-Pfalz: Energieversorgung rückt bei Bedrohungen stärker in den Fokus (19.10.)**

Relevanz: MITTEL

Laut Innenminister Achim Schwickert (Antwort auf eine parlamentarische Anfrage) rücken die Energieversorgung, militärische Einrichtungen sowie Rüstungsunternehmen und deren Dienstleister in den Fokus, Einrichtungen der kritischen Infrastruktur seien einer erhöhten Gefährdung ausgesetzt. Genannt werden physische Angriffe wie Sachbeschädigung und Brandstiftung sowie Angriffe aus dem Cyberraum. Seit 2024 bis Ende September 2026 wurden 13 politisch motivierte Straftaten gegen Infrastruktur, Militär, Justiz sowie Handel und Wirtschaft erfasst, die meisten gegen Militäranlagen. Für Versorger in DACH ist das ein Anlass, physische Sicherheit und OT-Sicherheit gemeinsam zu planen.

Quelle:
https://www.heise.de/news/Drohnenfluege-und-Cyberattacken-Behoerden-beraten-Firmen-11491990.html

L-05 **Ransomware-Gruppe Settra listet deutschen Anlagenbauer aus der Abwassertechnik (unbestätigt)** Seit spätestens 18.10. ist ein deutscher Anlagenbauer aus der Abwassertechnik auf der Leak-Site der Ransomware-Gruppe „Settra“ gelistet. An diesem Tag hat ransomware.live den Eintrag erfasst. Die Täter behaupten, 140 GB Daten erbeutet zu haben. Den Angriff schätzt ransomware.live auf etwa den 25.09. **Unbestätigt, nur laut Täterangabe:** Eine Stellungnahme der Firma, einer Behörde oder einen Medienbericht haben wir bis zum 20.10. nicht gefunden. Deshalb nennen wir den Namen nicht und verlinken den Leak-Eintrag nicht. Einschätzung: Typischerweise können bei Anlagenbauern für Kläranlagen Projekt- und Automatisierungsunterlagen, Zugänge für die Fernwartung und Kundenlisten von Betreibern liegen. Ob solche Daten hier betroffen sind, ist nicht bekannt. Betreiber, die mit Anlagenbauern aus diesem Bereich arbeiten, sollten prüfen, welche Fernwartungszugänge der Dienstleister hat, und diese bei Bedarf neu vergeben (CC4 Secure Remote Access). Quellen: https://www.ransomware.live/group/settra

Relevanz: HOCH

L-06 UPDATE: **Update: Loxone bestätigt kopierte CRM-Daten, Erpresserschreiben nennt 201,6 GB (19.10.) Laut heise (19.10.) hat Loxone bestätigt, dass Daten kopiert wurden, vor allem aus dem CRM-System (Kontaktdaten von Partnerbetrieben, Supportanfragen) und aus dem Bewerbermanagement. Zu der Datenmenge äußert sich Loxone nicht. Miniserver, Remote Connect und Exosphere sind laut Loxone nicht betroffen, Benutzer- und Zugangsdaten liegen nach Angaben des Herstellers nur lokal am Miniserver. Unbestätigt ist das Erpresserschreiben, das Borns IT-Blog zeigt: Die Angreifer behaupten, 201,6 GB kopiert und verschlüsselt zu haben, und drohen mit Veröffentlichung in etwa drei Tagen (Stand 19.10.). Im Zusammenhang mit veröffentlichten Beispieldaten weist Loxone darauf hin, dass loxwiki nicht von Loxone betrieben wird und nicht auf einer Loxone-Domain läuft. Dass die Ticketing-Plattform teilweise betroffen sei, steht nur in einem Leserkommentar bei Born mit Verweis auf das Loxforum; Loxone selbst nennt kopierte Supportanfragen. Vorsorgliche Empfehlung von uns, nicht von Loxone: Wer Zugangsdaten, API-Zugänge oder Konfigurationen in Supportanfragen an Loxone geschickt hat, sollte diese erneuern. Quellen: https://www.heise.de/news/Loxone-Cyberangriff-auf-Gebaeudeautomatisierungsanbieter-11492872.html , https://borncity.com/blog/2026/10/19/sicherheitsvorfall-bei-loxone/ (Erstmeldung am 19.10.2026: https://ot-cyber.de/ot-lage/2026-10-19.html)**

Relevanz: MITTEL

L-07 **Claroty Team82: KI-Agent baut root-Exploit für Danfoss AK-SM 800A in rund 28 Minuten nach Claroty Team82 hat am 13.10. gezeigt, wie Claude Sonnet 4.6 (mittlerer Reasoning-Modus, im Editor Cursor) bekannte Lücken in der Kühlstellensteuerung Danfoss AK-SM 800A nachbaut. Eigene Forschungsergebnisse von Team82 bekam die KI nicht. Als Eingaben dienten öffentliche CVE-Angaben und Schwachstellenklassen, die frei herunterladbare Firmware und Analysewerkzeuge. Der Agent verkettete zwei der Lücken zur Ausführung von Befehlen als root auf einem Laborgerät. Von der ersten Analyse bis zum funktionierenden Exploit vergingen etwa 28 Minuten, die KI-Nutzung kostete rund 6 US-Dollar. Ganz ohne Menschen ging es nicht: Am Authentication Bypass scheiterte der Agent zunächst. Forscher lenkten die Analyse um und stellten eine Ghidra-Anbindung für das 67 MB große Hauptprogramm bereit. Im früheren Bericht vom 09.08. nennt Claroty 2.765 aus dem Internet erreichbare Geräte laut Censys und die von Danfoss veröffentlichte Firmware R4.3.1. Laut NeoTeo behebt diese Version nach Angaben von Claroty die bekannten Lücken. Unsere Einschätzung: Wenn, wie im Laborversuch, zu einer bekannten Lücke in einer halben Stunde ein Exploit steht, zählt bei OT-Geräten im Internet jeder Tag ohne Patch. Steuerungen gehören nicht direkt ins Internet (CC5 Risk-Based Vulnerability Management). Es ist ein Laborversuch und kein neuer Vorfall. Ob dieser Angriffsweg bei Vorfällen in französischen Supermärkten genutzt wurde, ist laut Claroty nicht bestätigt. Quellen: https://claroty.com/team82/research/firmware-to-root-in-30-minutes-how-ai-is-changing-threat-intelligence , https://claroty.com/team82/research/freeze-the-controller-defrost-the-food-uncovering-vulnerabilities-in-danfoss-refrigeration-controllers , https://www.neoteo.com/en/claroty-says-claude-reproduced-danfoss-flaws-in-about-28-minutes , https://industrialcyber.co/ai/claroty-team82-shows-ai-can-rebuild-danfoss-controller-exploits-in**

Relevanz: MITTEL

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