

WOCHENBERICHT

OT-/Cyber-Lagebild Gesamt

Ausgabe KW 43/2026 · Gesamt – alle OT-Branchen in DACH

Zielgruppe	Betreiber von Anlagen und Maschinen, KRITIS, Industrie in DACH
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 Betreiber von Anlagen und Maschinen, KRITIS, Industrie in DACH in Deutschland, Österreich und der Schweiz.

Management Summary

Rund um den Berichtszeitraum (15. bis 23.10.) stehen Fernzugänge und Edge Devices im Vordergrund. BeyondTrust Remote Support wurde vor der Veröffentlichung als Zero-Day ausgenutzt; die zwei bekannten Kompromittierungen datiert BeyondTrust auf den 29.08. Laut Rapid7 ordnet Mandiant die Aktivität dem mutmaßlich China-nahen Spionageakteur ARMORY CASTLE (früher UNC5221) zu. Die Lücke wurde am 15.10. veröffentlicht und am 16.10. in den KEV-Katalog aufgenommen. Arista hat einen weiteren ausgenutzten Zero-Day im VeloCloud Orchestrator geschlossen. FBI, CISA, US Secret Service, LKA Rheinland-Pfalz sowie die britische National Crime Agency und die North West Regional Organised Crime Unit warnen gemeinsam vor SafePay. Von der Ransomware-Gruppe sind seit August 2024 mindestens 600 Organisationen aus mehreren Sektoren kritischer Infrastruktur betroffen. Der Zugang läuft laut Advisory über gestohlene oder erratene Passwörter, ausgenutzte Schwachstellen und Phishing.

In der Automatisierung selbst gibt es ein wichtiges Advisory. Bei den Webservern von SIMATIC S7-1500 und ET 200SP (zahlreiche Produkte, CVSS bis 9,6) gibt es für einen großen Teil der Produkte noch keinen Fix; Siemens bereitet Fixes vor und empfiehlt bis dahin Gegenmaßnahmen. Dazu kommt das Siemens Software Center: Laut The Hacker News bringen Angreifer selbst eine echte, signierte ältere Kopie (laut Siemens war 3.5.8.7 damals aktuell) samt archive.dll per MSI über einen ClickFix-Köder mit, um einen Remote Access Trojan einzuschleusen. Gefährdet ist, wer den ClickFix-Köder ausführt; Siemens empfiehlt das Update auf 4.0.9.8 und laut The Hacker News zusätzlich, die IoCs zu sperren und nach SiemensSoftwareCenter.exe in AppData\Local\Programs zu suchen, die von msixexec.exe gestartet wurde. Beim Hersteller Loxone waren laut Loxone interne Systeme, das CRM mit Partnerdaten und Bewerberdaten betroffen; laut Loxone gab es weltweit keine Vorkommnisse bei Kundeninstallationen und keinen Zugriff auf Kundeninstallationen.

GESAMTBEWERTUNG

Die Lage ist hoch, weil mehrere Zero-Days in Fernwartungs- und WAN-Produkten aktiv ausgenutzt werden, die dort, wo sie als Fernwartungszugang genutzt werden, direkt vor der Leittechnik stehen. Zuerst kommen BeyondTrust (patchen, Zugangsdaten wechseln, Spuren suchen) und die Härtung der SPS-Webserver, für die es für einen großen Teil der Produkte noch keinen Fix gibt.

Trends

- Mutmaßlich China-nahe Spionagegruppen und Ransomware-Banden greifen gezielt Fernwartungs- und WAN-Produkte an (BeyondTrust, VeloCloud, Fortinet, PAN-OS), und ein Patch entfernt keine Angreifer, die schon im System sind.
- Angriffe auf Hersteller und Auftragnehmer treffen Betreiber über die Lieferkette: Bei Loxone sind Partnerdaten betroffen, beim Fehmarnbelt-Konsortium Femern Link Contractors waren seit dem 12.10. IT-Systeme auf der Baustelle gestört.
- Engineering-Software wird zum Malware-Träger: Beim Siemens Software Center bringen Angreifer eine signierte Programmdatei per ClickFix selbst mit.
- Für SPS-Webserver gibt es öfter Advisories ohne Patch, dann helfen nur Abschalten und Segmentierung.

- Für zwei kritische RCE-Lücken in PHP (CVE-2026-109618/-109619) sind Notfall-Patches erschienen, in PHP 8.5.12, 8.4.27, 8.3.36 und 8.2.35. Für 7.4, 8.0 und 8.1 hat das PHP-Team ausnahmsweise minimale Source-Backports bereitgestellt.

Lageübersicht

ID	Meldung	Relevanz	Quelle
L-01	BeyondTrust Remote Support: Zero-Day vor der Veröffentlichung ausgenutzt, KEV seit 16.10. (CVE-2026-102764)	KRITISCH	Rapid7 / Canadian Centre for Cyber Security / BleepingComputer, 16.10.
L-02	Siemens SIMATIC S7-1500 und ET 200SP: acht CVEs im Webserver (Typen laut CISA: Eval Injection und Cross-Site Scripting), für einen großen Teil der Produkte noch kein Fix (ICSA-26-295-14)	HOCH	CISA ICS Advisory, 22.10.
L-03	FBI, CISA, US Secret Service, LKA Rheinland-Pfalz und britische Behörden warnen vor SafePay-Ransomware (AA26-293A)	HOCH	CISA Joint Cybersecurity Advisory, 20.10.
L-05	Siemens Software Center: signierte Kopie wird für ClickFix-Malware missbraucht (CVE-2026-110936)	HOCH	Siemens ProductCERT, berichtet von The Hacker News / SOC Prime, 19.10.
L-06	Arista VeloCloud Orchestrator: neuer ausgenutzter Zero-Day im SD-WAN (CVE-2026-114625)	HOCH	BleepingComputer, 22.10.
L-07	Loxone: Cyberangriff auf interne Systeme, 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
Bayern (München)	1441	OMRON FINS: 771, HMI/VNC: 191, DNP3: 181, Siemens S7: 35, OPC UA: 20
Salzburg	27	HMI/VNC: 8, Niagara Fox: 5, BACnet: 4, Siemens S7: 2, OPC UA: 1
Tirol (Innsbruck)	47	HMI/VNC: 14, DNP3: 8, Niagara Fox: 6, Siemens S7: 2, OPC UA: 1

Meldungen im Detail

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

KRITISCH Rapid7 / Canadian Centre for Cyber Security / BleepingComputer, 16.10.

Was ist neu: Über eine Lücke in der Herkunftsprüfung (CWE-290, CVSS 4.0: 9,3) können Angreifer ohne Konto Dateioperationen auf der Appliance ausführen. Betroffen sind die Versionen 26.2.3 und älter. Laut Rapid7 ordnet Mandiant die Aktivität aus seiner Untersuchung ARMORY CASTLE zu, einem mutmaßlich China-nahen Spionageakteur (früher UNC5221). Die Gruppe legt die Webshell SAWFLY und den Tunneler BARECLAW ab, eskaliert auf root, versucht den Credential Vault auszulesen und löscht Logs. 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. Die Lücke wurde am 15.10. veröffentlicht, am 16.10. in den KEV-Katalog aufgenommen.

Bedeutung: Wo BeyondTrust als Fernwartungszugang genutzt wird, kommen Dienstleister darüber an Jump Hosts und Leittechnik. Wer die Appliance kontrolliert, kann nach unserer Einordnung auch an die dort gespeicherten Zugangsdaten zur OT kommen. Mandiant rechnet nach der Veröffentlichung mit breiter, opportunistischer Ausnutzung.

Empfehlung: Selbst betriebene Appliances sofort patchen. Bei Versionen vor 24.3.1 zuerst upgraden. 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. Rapid7 empfiehlt, auch nach dem Patch auf Kompromittierung zu prüfen. Hinterlegte Zugangsdaten zu OT-Systemen wechseln und mit den IoCs von Mandiant und Rapid7 nach Spuren suchen.

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 (Typen laut CISA: Eval Injection und Cross-Site Scripting), für einen großen Teil der Produkte noch kein Fix (ICSA-26-295-14)

HOCH CISA ICS Advisory, 22.10.

Was ist neu: Das CISA-Advisory vom 22.10. nennt CVE-2026-63350 bis CVE-2026-63357 für zahlreiche Siemens-Produkte, darunter S7-1500, ET 200SP, ET 200pro, Software Controller und PLCSIM Advanced. Die höchste Bewertung ist CVSS v3 9,6. Es handelt sich um acht CVEs (Typen laut CISA: Eval Injection und Cross-Site Scripting): Schadcode läuft in der Browser-Sitzung eines berechtigten Nutzers. Angreifer können damit SPS-Operationen im Rahmen der Rechte des angemeldeten Nutzers ausführen. 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, nach unserer Einordnung auch in Wasser, Energie und Fertigung in DACH. Der Webserver ist in vielen Projekten für Diagnose eingeschaltet. Bis zum Fix empfiehlt Siemens, den Webserver abzuschalten, wo er nicht gebraucht wird, den Zugriff auf Port 80/443 auf vertrauenswürdige IP-Adressen zu beschränken und nur vertrauenswürdige Trace-Dateien hochzuladen.

Empfehlung: Im Asset-Inventar prüfen, auf welchen CPUs der Webserver aktiv ist, und ihn abschalten, wo er nicht gebraucht wird. Sonst den Zugriff auf 80/443 per Firewall auf Engineering-Netze begrenzen und das Team anweisen, nur vertrauenswürdige Trace-Dateien hochzuladen.

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

L-03 FBI, CISA, US Secret Service, LKA Rheinland-Pfalz und britische Behörden warnen vor SafePay-Ransomware (AA26-293A)

HOCH CISA Joint Cybersecurity Advisory, 20.10.

Was ist neu: 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 beruht auf Ermittlungen von FBI, US Secret Service (USSS) und LKA Rheinland-Pfalz. Von SafePay sind seit August 2024 mindestens 600 Organisationen aus mehreren Sektoren kritischer Infrastruktur betroffen, auch in Europa. Der Initial Access läuft laut Advisory über gestohlene oder erratene Passwörter, ausgenutzte Schwachstellen und Phishing. Genannt werden CVE-2020-3259, CVE-2023-20269, CVE-2023-27532, CVE-2024-40711 und CVE-2024-40766. Nach unserer Einordnung betreffen die CVEs u. a. VPN-Systeme und Veeam Backup. Danach schalten die Angreifer Sicherheitsfunktionen ab, um unentdeckt zu bleiben.

Bedeutung: Ein deutsches LKA ermittelt mit, das deutet nach unserer Einordnung auf Opfer in Deutschland hin. Die genannten Lücken stecken laut NVD in Cisco ASA/FTD, Veeam Backup & Replication und SonicWall SonicOS, also in Produkten, die auch Mittelständler und Stadtwerke betreiben. Fällt das Backup, verlängert sich der Ausfall auch für OT-nahe Systeme.

Empfehlung: Patchstand der fünf CVEs auf Firewalls, VPN und Veeam-Servern prüfen. MFA für jeden VPN-Zugang erzwingen und für OT-relevante Systeme ein Offline-Backup bereithalten, dessen Wiederherstellung schon getestet wurde.

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

L-05 Siemens Software Center: signierte Kopie wird für ClickFix-Malware missbraucht (CVE-2026-110936)

HOCH Siemens ProductCERT, berichtet von The Hacker News / SOC Prime, 19.10.

Was ist neu: Siemens hat eine DLL-Sideloadung-Lücke (CVSS v4 8,4) geschlossen, die laut Siemens in ClickFix-Angriffen ausgenutzt wird. Laut The Hacker News bringen die Angreifer selbst eine echte, signierte ältere Kopie des Software Center (laut Siemens war 3.5.8.7 damals aktuell) samt archive.dll per MSI über einen ClickFix-Köder mit, um Schadcode auszuführen; laut Huntress wird am Ende ein Remote Access Trojan installiert. Version 4.0.9.8 schließt die Lücke, das Update wird beim Start der Anwendung eingespielt. Siemens empfiehlt das Update auf 4.0.9.8 und laut The Hacker News zusätzlich, die IoCs zu sperren und nach SiemensSoftwareCenter.exe in AppData\Local\Programs zu suchen, die von msiexec.exe gestartet wurde.

Bedeutung: Gefährdet ist, wer den ClickFix-Köder ausführt; Siemens empfiehlt das Update auf 4.0.9.8 und laut The Hacker News zusätzlich, die IoCs zu sperren und nach SiemensSoftwareCenter.exe in AppData\Local\Programs zu suchen, die von msiexec.exe gestartet wurde. Eine signierte Datei fällt bei vielen Endpoint-Lösungen weniger auf.

Empfehlung: Windows- und Engineering-PCs auf ClickFix- und MSI-Ausführungen prüfen und auf SiemensSoftwareCenter.exe in AppData\Local\Programs, die von msiexec.exe gestartet wurde. Außerdem die Version prüfen und mit den IoCs von Siemens suchen: Ordner „SM Software Provisioning Service“ unter AppData\Local\Programs, Dateien activate.bak und statinfosta.DB, Verbindungen zu 96.62.218[.]59 und wizardexpensive[.]com. Die IoCs an Firewall und Proxy sperren.

Quelle: <https://thehackernews.com/2026/10/clickfix-attackers-exploit-siemens.html> ✓ geprüft

L-06 Arista VeloCloud Orchestrator: neuer ausgenutzter Zero-Day im SD-WAN (CVE-2026-114625)

HOCH BleepingComputer, 22.10.

Was ist neu: Über eine SQL-Injection kann jedes angemeldete Konto mit Basisrechten (basic privileges) und gültiger Sitzung auf der VCO-Weboberfläche Operator-Rechte bekommen und sich als lokaler „superuser operator“ ausgeben. Die Lücke wird bereits ausgenutzt. Arista nennt die Angreifer-IPs 74.82.197.86 und 38.54.50.151. Schon im Juli wurde eine andere VCO-Lücke ausgenutzt (CVE-2026-16812).

Bedeutung: Wer den Orchestrator übernimmt, steuert die WAN-Verbindungen aller angebundenen Standorte. Das kann die Segmentierung zwischen Außenstationen und Zentrale aushebeln.

Empfehlung: On-Prem-Orchestrator sofort patchen und das Web-Interface nur aus dem Management-Netz erreichbar lassen. Vor dem Patch Logs sichern und die Admin-Aktivität der letzten Wochen auf ungewöhnliche Anmeldungen prüfen.

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

L-07 Loxone: Cyberangriff auf interne Systeme, laut Loxone weltweit keine Vorkommnisse bei Kundeninstallationen

MITTEL Loxone-Sicherheitsseite, 19.10.

Was ist neu: Laut Loxone richtete sich ein Cyberangriff gegen interne Unternehmenssysteme, insbesondere CRM-Systeme mit Daten der Partnerbetriebe sowie Bewerberdaten. Laut Loxone gab es weltweit keine Vorkommnisse bei Kundeninstallationen und keinen Zugriff auf Kundeninstallationen. Loxone führt Zwei-Faktor-Authentifizierung ein.

Bedeutung: Nach unserer Einschätzung steuert Loxone in DACH viele kommunale und gewerbliche Gebäude. Nach unserer Einschätzung lässt sich mit Kontaktdaten der Installateure glaubwürdiges Phishing an Betreiber schicken, etwa als angebliches Update oder Support-Anfrage.

Empfehlung: Betreiber von Loxone-Anlagen sollten eingehende Mails mit Loxone- oder Installateurbezug besonders prüfen und Fernzugänge der Installateure auf MFA und aktuelle Passwörter kontrollieren.

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

Empfehlungen

Nr.	Maßnahme	Bezug	Priorität	Zeitraum
M-01	BeyondTrust patchen, hinterlegte OT-Zugangsdaten wechseln und eine Kompromittierungsprüfung durchführen [CC4 Secure Remote Access]	L-01	HOCH	sofort
M-02	Webserver der Siemens-SPS abschalten oder per Firewall auf Engineering-Netze begrenzen, bis Siemens Fixes liefert [CC2 Defensible Architecture]	L-02	HOCH	sofort
M-03	VPN- und Edge-Device-Inventar gegen die CVEs aus AA26-293A abgleichen, MFA für alle Fernzugänge durchsetzen [CC5 Risk-Based Vulnerability Management]	L-03	HOCH	0 bis 3 Monate

Nr.	Maßnahme	Bezug	Priorität	Zeitraum
M-05	Windows- und Engineering-PCs in die Angriffserkennung aufnehmen (EDR- und Netzwerk-Logs ins SIEM) und Ablauf für IoC-Suchen festlegen [CC3 ICS Network Visibility & Monitoring]	L-05	MITTEL	3 bis 6 Monate

Fragen für das nächste Jour fixe

1. Nutzen wir oder unsere Dienstleister BeyondTrust Remote Support, und welche OT-Zugangsdaten liegen dort?
2. Auf welchen S7-1500- und ET-200SP-CPUs ist der Webserver aktiv, und wer braucht ihn wirklich?
3. Ist MFA an jedem VPN-Zugang Pflicht, auch für Dienstleister und Servicekonten?
4. Haben wir ein Offline-Backup der OT-Projekte und Engineering-Daten, dessen Wiederherstellung schon getestet wurde?

Maßnahmen dieser Woche

1. BeyondTrust-Appliances patchen (BT26-05), alle dort hinterlegten Zugangsdaten zu Jump Hosts und Leittechnik wechseln und IoCs prüfen.
2. SPS-Webserver der S7-1500/ET 200SP abschalten oder Ports 80/443 auf Engineering-Netze begrenzen.
3. Windows- und Engineering-PCs auf ClickFix/MSI-Ausführungen, von msixexec.exe gestartete SiemensSoftwareCenter.exe in AppData\Local\Programs und die Siemens-IoCs prüfen, IoCs an der Firewall sperren.
4. VPN, Firewalls und Veeam-Server gegen die fünf CVEs aus AA26-293A abgleichen und MFA am VPN kontrollieren.
5. VeloCloud Orchestrator (On-Prem) patchen und die Admin-Logs auf die Arista-IPs prüfen.

HINWEIS ZUR QUELLENLAGE

Geprüft an Primärquellen: AA26-293A und ICSA-26-295-14 bei CISA, die Loxone-Pressemitteilung, Arista über BleepingComputer und BeyondTrust über Rapid7 und das kanadische Cyber Centre. Nicht aufgenommen: WAGO ICSA-26-293-02 / VDE-2026-096, weil die CISA-Seite und die Seite von CERT@VDE beim Abruf nicht erreichbar waren. Siemens SSA-580366 ist an der Herstellerangabe geprüft (CVSS v4 8,4, Fix 4.0.9.8). Nicht aufgenommen, weil unbestätigt: Settra-Leak zu Passavant Energy & Environment (nur Täterangaben, keine Presse- oder Firmenbestätigung gefunden), die Leak-Behauptungen der Gruppe „Samurai“ zu Loxone (M365/SSO, Miniserver-Seriennummern) und die Zuordnung von PAN-OS CVE-2026-0257 zu Settra und zum Sektor Versorger (belegt ist nur Qilin über Arctic Wolf). Eclipse Milo (ICSA-26-288-01) ist an der CISA-Seite geprüft und wurde dort am 15.10. veröffentlicht. Die Zahl der Betroffenen des österreichischen NISG 2026 (seit 01.10.) schwankt je nach Quelle zwischen rund 4.000 und 5.000. 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.