

**WOCHENBERICHT**

# OT-/Cyber-Lagebild Maschinen- und Anlagenbau

Ausgabe KW 43/2026 · Maschinen- und Anlagenbau in DACH

|                         |                                                                        |
|-------------------------|------------------------------------------------------------------------|
| <b>Zielgruppe</b>       | Maschinen- und Anlagenbauer, Komponentenhersteller, Systemintegratoren |
| <b>Berichtszeitraum</b> | 16.10.2026–23.10.2026                                                  |
| <b>Version</b>          | 1.0                                                                    |
| <b>Datum</b>            | 23.10.2026                                                             |
| <b>Autor</b>            | Maximilian Gilg, OT-Cyber.de                                           |
| <b>Klassifizierung</b>  | TLP:CLEAR – ausschließlich öffentliche Quellen                         |

Dieser Bericht fasst öffentlich zugängliche Meldungen zusammen. Die Einstufung der Relevanz bezieht sich auf Maschinen- und Anlagenbauer, Komponentenhersteller, Systemintegratoren in Deutschland, Österreich und der Schweiz.

## Management Summary

Im Berichtszeitraum (16. bis 23.10.) sind die wichtigsten Meldungen für den Maschinen- und Anlagenbau neue Schwachstellen in den Produkten selbst. Siemens meldet acht CVEs (Typen laut CISA: Eval Injection und Cross-Site Scripting) im Webserver von SIMATIC S7-1500 und ET 200SP. Angreifer können damit SPS-Operationen im Rahmen der Rechte des angemeldeten Nutzers ausführen. Betroffen sind zahlreiche Produkte in allen Versionen, der höchste CVSS-Wert liegt bei 9,6. Für einen großen Teil der Produkte gibt es noch keinen Fix; Siemens bereitet Fixes vor und empfiehlt bis dahin Gegenmaßnahmen. Beim Siemens Software Center bringen die Angreifer laut The Hacker News 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. Gefährdet ist, wer den ClickFix-Köder ausführt. Siemens empfiehlt das Update auf 4.0.9.8; laut The Hacker News empfiehlt der Siemens-Hinweis zudem IoC-Sperren und die Suche nach SiemensSoftwareCenter.exe in AppData\Local\Programs, gestartet von msixexec.exe.

Bei der Fernwartung bleibt die Lage angespannt. BeyondTrust Remote Support wurde vor der Veröffentlichung ausgenutzt; die Lücke wurde am 15.10. veröffentlicht, am 16.10. in den KEV-Katalog aufgenommen. Die zwei bekannten Kompromittierungen datiert BeyondTrust auf den 29.08. Laut Rapid7 ordnet Mandiant die Aktivität aus seiner Untersuchung ARMORY CASTLE zu, einem mutmaßlich China-nahen Spionageakteur (früher UNC5221). 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. Laut Advisory sind seit August 2024 mindestens 600 Organisationen aus mehreren Sektoren kritischer Infrastruktur betroffen; Zugang verschaffen sich die Täter über gestohlene oder erratene Passwörter, ausgenutzte Schwachstellen und Phishing. Bei Loxone traf ein Cyberangriff interne Unternehmenssysteme, insbesondere CRM-Systeme mit Daten der Partnerbetriebe sowie Bewerberdaten. Laut Loxone gibt es weltweit keine Vorkommnisse bei Kundeninstallationen und keinen Zugriff auf Kundeninstallationen. Hersteller, die von einer aktiv ausgenutzten Schwachstelle in ihrem Produkt erfahren, müssen seit dem 11.09.2026 nach Art. 14 CRA (Verordnung (EU) 2024/2847) innerhalb von 24 Stunden eine Frühwarnung abgeben.

### GESAMTBEWERTUNG

Die Lage ist erhöht bis hoch, weil Steuerungslücken, für die es großteils noch keinen Fix gibt, und aktiv ausgenutzte Fernwartungs- und Engineering-Software zusammenkommen. Vorrang haben die Prüfung der BeyondTrust-Appliances, die Prüfung der Windows- und Engineering-PCs auf ClickFix/MSI-Ausführungen mit Siemens Software Center und die Absicherung der S7-1500-Webserver in ausgelieferten Anlagen.

## Trends

- Der Mensch wird zum Einfallstor: Beim Siemens Software Center (signierte Programmdatei mit ClickFix-Köder) braucht der Angreifer ein Opfer, das mitmacht, bei den S7-1500-Webserver-Lücken laufen die Angriffe im Browser des Nutzers.
- Fernwartungsplattformen wie BeyondTrust bleiben ein Hauptziel, im aktuellen Fall laut Rapid7 nach Zuordnung von Mandiant eines mutmaßlich China-nahen Spionageakteurs. Rapid7 rät, auch nach dem Patch auf Kompromittierung zu prüfen (<https://www.rapid7.com/blog/post/etr-cve-2026-102764-critical-beyondtrust-remote-support-authentication-bypass-exploited-in-the-wild>).

- Angriffe auf Hersteller und Auftragnehmer treffen die Kunden: Bei Loxone sind es Partnerdaten, beim Fehmarnbelt-Tunnel fielen laut heise Zutrittskarten, Bauschiffe mit präziser Positionierung und Kräne aus (<https://www.heise.de/news/Nach-Cyberangriff-Bauarbeiten-am-Fehmarnbelt-Tunnel-gestoert-11490277.html>).
- Bibliotheken in Produkten werden zum SBOM-Thema: Eclipse Milo (OPC UA, ICSA-26-288-01 vom 15.10.) ist behoben ab Version 1.1.5; für 0.6.x gibt es keinen Fix (<https://www.cisa.gov/news-events/ics-advisories/icsa-26-288-01>).
- Seit dem 11.09.2026 gelten die CRA-Meldepflichten über die ENISA Single Reporting Plattform: Frühwarnung innerhalb von 24 Stunden, Meldung nach 72 Stunden, Abschlussbericht 14 Tage nach der Abhilfe (<https://helpnetsecurity.com/2026/09/14/enisa-cra-single-reporting-platform>).

## Lageübersicht

| ID   | Meldung                                                                                                            | Relevanz | Quelle                                                                            |
|------|--------------------------------------------------------------------------------------------------------------------|----------|-----------------------------------------------------------------------------------|
| L-01 | Siemens SIMATIC S7-1500 und ET 200SP: acht CVEs im Webserver, für viele Produkte noch kein Fix (ICSA-26-295-14)    | KRITISCH | CISA / Siemens ProductCERT, 22.10.                                                |
| L-02 | BeyondTrust Remote Support: Zero-Day vor der Veröffentlichung ausgenutzt, KEV seit 16.10. (CVE-2026-102764)        | KRITISCH | Rapid7 / BleepingComputer / Canadian Centre for Cyber Security / Mandiant, 16.10. |
| L-03 | Siemens Software Center wird über ClickFix-Köder ausgenutzt (CVE-2026-110936)                                      | HOCH     | The Hacker News / Siemens ProductCERT, 20.10.                                     |
| L-04 | Loxone: Cyberangriff auf interne Systeme, CRM- und Bewerberdaten betroffen                                         | HOCH     | Loxone ( <a href="https://security.loxone.com">security.loxone.com</a> ), 22.10.  |
| L-05 | FBI, CISA, US Secret Service, LKA Rheinland-Pfalz und britische Behörden warnen vor SafePay-Ransomware (AA26-293A) | HOCH     | CISA, 20.10.                                                                      |
| L-06 | Weitere ICS-Advisories: Moxa AIG-302 mit hart codiertem Schlüssel                                                  | MITTEL   | CISA, 20.10.                                                                      |

## 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            |

## Meldungen im Detail

### **L-01 Siemens SIMATIC S7-1500 und ET 200SP: acht CVEs im Webserver, für viele Produkte noch kein Fix (ICSA-26-295-14)**

KRITISCH CISA / Siemens ProductCERT, 22.10.

Was ist neu: Das CISA-Advisory vom 22.10. veröffentlicht das Siemens-Advisory zu CVE-2026-63350 bis CVE-2026-63357. Betroffen sind zahlreiche Produkte aus den Reihen S7-1500, ET 200SP, Drive Controller, Software Controller, PLCSIM Advanced und SIPLUS, jeweils in allen Versionen, mit CVSS v3 bis 9,6. Die Lücken ermöglichen Angriffe im Browser des Nutzers (Cross-Site Scripting): Ein Angreifer kann Schadcode in der Browsersitzung eines berechtigten Nutzers ausführen und SPS-Aktionen im Rahmen von dessen Rechten durchführen. Siemens rät u. a., nur vertrauenswürdige Trace-Dateien hochzuladen.

Bedeutung: Die S7-1500 ist eine weit verbreitete SPS-Familie und steckt in vielen ausgelieferten Maschinen. Bis Fixes kommen, muss der Maschinenbauer die Kunden aktiv informieren, sonst bleiben die Webserver im Feld offen. Unter dem CRA zählt das zur Pflicht, Schwachstellen über den Lebenszyklus zu behandeln, auch bei Komponenten von Zulieferern.

Empfehlung: Im Asset-Inventar bzw. in der Installed Base prüfen, wo der CPU-Webserver aktiv ist, und ihn abschalten, wo er nicht gebraucht wird. Service-Techniker anweisen, nur vertrauenswürdige Trace-Dateien hochzuladen, und Kunden mit einem kurzen Security-Hinweis versorgen (CC5 Risk-Based Vulnerability Management).

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

## **L-02 BeyondTrust Remote Support: Zero-Day vor der Veröffentlichung ausgenutzt, KEV seit 16.10. (CVE-2026-102764)**

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

Was ist neu: Die Lücke wurde am 15.10. veröffentlicht, am 16.10. in den KEV-Katalog aufgenommen. Ohne Konto lässt sich die Authentifizierung umgehen, CVSS 4.0 9,3. Betroffen sind die Versionen 26.2.3 und älter. Ausgenutzt wurde die Lücke vor der Veröffentlichung; die zwei bekannten Kompromittierungen, eine gehostete Instanz und eine selbst betriebene Appliance, datiert BeyondTrust auf den 29.08.2026. Laut Rapid7 ordnet Mandiant die Aktivität aus seiner Untersuchung ARMORY CASTLE zu, einem mutmaßlich China-nahen Spionageakteur (früher UNC5221).

Bedeutung: Wo BeyondTrust als Fernwartungszugang zu Kundenanlagen genutzt wird, kann eine kompromittierte Appliance den Weg zu Jump Hosts und Steuerungsnetzen der Kunden öffnen. Mandiant beobachtete laut Rapid7 den Versuch, den Credential Vault auszulesen. Laut Rapid7 sollten gespeicherte oder vermittelte Zugangsdaten nach Patch oder Neuaufbau gewechselt und administrative Änderungen geprüft werden. Damit wird der Hersteller selbst zum Weg in die Lieferkette.

Empfehlung: Selbst gehostete Appliances sofort patchen (vor 24.3.1 erst ein Upgrade). Rapid7 empfiehlt, auch nach dem Patch auf Kompromittierung zu prüfen. 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. Alle dort gespeicherten Zugangsdaten für Kundenanlagen wechseln und die betroffenen Kunden informieren (CC4 Secure Remote Access, CC1 ICS Incident Response).

Quelle: <https://www.rapid7.com/blog/post/etr-cve-2026-102764-critical-beyondtrust-remote-support-authentication-bypass-exploited-in-the-wild/> ✓ geprüft

## **L-03 Siemens Software Center wird über ClickFix-Köder ausgenutzt (CVE-2026-110936)**

HOCH The Hacker News / Siemens ProductCERT, 20.10.

Was ist neu: Siemens hat die DLL-Sideloadung-Lücke (CVSS v4 8,4) in Version 4.0.9.8 geschlossen. Laut The Hacker News bringen die Angreifer über einen ClickFix-Köder selbst eine echte, signierte ältere Kopie des Software Center (laut Siemens war 3.5.8.7 damals aktuell) samt präparierter „archive.dll“ per MSI mit. Dabei startet „msiexec.exe“ die Datei „AllMyBasic.msi“, die SiemensSoftwareCenter.exe ausführt. Laut Huntress wird am Ende ein Remote Access Trojan installiert.

Bedeutung: Gefährdet ist, wer den ClickFix-Köder ausführt, denn die Angreifer bringen die verwundbare Altversion selbst mit. Siemens empfiehlt das Update auf 4.0.9.8; laut The Hacker News empfiehlt der Siemens-Hinweis zudem IoC-Sperren und die Suche nach SiemensSoftwareCenter.exe in AppData\Local\Programs, gestartet von msiexec.exe. Ein infizierter Service-Laptop wird so zum Weg in die Anlage beim Kunden. Weil die Datei korrekt signiert ist, hilft eine Prüfung nach Hash oder Signatur hier wenig.

Empfehlung: Windows- und Engineering-PCs auf ClickFix/MSI-Ausführungen und auf SiemensSoftwareCenter.exe in AppData\Local\Programs prüfen, die von msiexec.exe gestartet wurde. Die IoCs 96.62.218[.]59, wizardexpensive[.]com und 2.27.248[.]127 in Proxy und Firewall sperren und eigene Installationen auf Version 4.0.9.8 bringen (CC3 ICS Network Visibility & Monitoring).

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

## **L-04 Loxone: Cyberangriff auf interne Systeme, CRM- und Bewerberdaten betroffen**

**HOCH** Loxone (security.loxone.com), 22.10.

Was ist neu: Laut der Loxone-Sicherheitsseite richtete sich der Cyberangriff gegen interne Unternehmenssysteme, insbesondere CRM-Systeme mit Daten der Partnerbetriebe sowie Bewerberdaten. Laut Loxone gibt es weltweit keine Vorkommnisse bei Kundeninstallationen und keinen Zugriff auf Kundeninstallationen. Loxone führt eine Zwei-Faktor-Authentifizierung (2FA) ein.

Bedeutung: Nach unserer Einschätzung zeigt der Fall, dass ein Angriff auf einen Komponentenhersteller auch ohne direkten OT-Schaden das Partnernetz betrifft: CRM-Daten von Partnerbetrieben liefern Angreifern mögliche Ziele für Phishing. Nach unserer Einschätzung hat jeder Hersteller mit Partnernetz und CRM dasselbe Risiko.

Empfehlung: Eigene Ticket- und CRM-Systeme nach Passwörtern im Klartext durchsuchen und diese Zugangsdaten wechseln. Für Service-Einsätze persönliche, zeitlich begrenzte Konten statt geteilter Admin-Passwörter einführen und Konten mit 2FA absichern (CC4 Secure Remote Access).

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

## **L-05 FBI, CISA, US Secret Service, LKA Rheinland-Pfalz und britische Behörden warnen vor SafePay-Ransomware (AA26-293A)**

**HOCH** CISA, 20.10.

Was ist neu: Herausgeber des gemeinsamen Advisories sind FBI, CISA, US Secret Service, LKA Rheinland-Pfalz sowie die britische National Crime Agency und die North West Regional Organised Crime Unit. Laut Advisory sind seit August 2024 mindestens 600 Organisationen aus mehreren Sektoren kritischer Infrastruktur betroffen, auch in Europa. Den Einstieg finden die Täter 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. Die Ermittlungen führen FBI, USSS und das LKA Rheinland-Pfalz.

Bedeutung: Mit dem LKA Rheinland-Pfalz ist eine deutsche Behörde an den Ermittlungen beteiligt, nach unserer Einschätzung ein Hinweis auf Opfer in DACH. Nach unserer Einordnung betreffen die genannten CVEs u. a. Firewalls, VPN-Systeme und Veeam Backup, wie sie auch im Mittelstand des Maschinenbaus stehen. Fällt die IT aus, stehen bei Herstellern auch Konstruktion, ERP und Fertigung still.

Empfehlung: Die fünf CVEs gegen das eigene Asset-Inventar abgleichen, MFA an allen VPN-Zugängen erzwingen und Konten nach Fehlversuchen sperren. Offline-Backups von Konstruktions- und Projektdaten wiederherstellen und den Ablauf dabei testen (CC1 ICS Incident Response).

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

## L-06 Weitere ICS-Advisories: Moxa AIG-302 mit hart codiertem Schlüssel

MITTEL CISA, 20.10.

Was ist neu: Moxa AIG-302 mit ThingsPro Edge bis 1.4.0 hat einen hart codierten kryptografischen Schlüssel (CVE-2026-109813, CVSS v3.1 8,1) und eine fehlende Autorisierung (6,8). Der Fix ist Firmware 1.4.1 (MPSA-262560).

Bedeutung: AIG-302-Gateways werden für die Anbindung von Maschinen an die Cloud verbaut, ein hart codierter Schlüssel gilt dann für alle Geräte im Feld.

Empfehlung: Ausgelieferte AIG-302 erfassen und das Update an die Kunden geben (CC5 Risk-Based Vulnerability Management).

Quelle: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-293-03> ✓ geprüft

## Empfehlungen

| Nr.  | Maßnahme                                                                                                                                                                                                                                                  | Bezug | Priorität | Zeitraum       |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-----------|----------------|
| M-01 | BeyondTrust/Fernwartungs-Appliances patchen, auf Kompromittierung prüfen, Kunden-Zugangsdaten wechseln [CC4 Secure Remote Access]                                                                                                                         | L-02  | HOCH      | sofort         |
| M-02 | Webserver der S7-1500/ET 200SP in der Installed Base abschalten oder einschränken und Kunden informieren [CC5 Risk-Based Vulnerability Management]                                                                                                        | L-01  | HOCH      | sofort         |
| M-03 | Windows- und Engineering-PCs prüfen: EDR-Suche nach ClickFix/MSI-Ausführungen und SiemensSoftwareCenter.exe aus AppData\Local\Programs mit msixexec.exe als Startprozess, IoCs sperren, Software Center 4.0.9.8 [CC3 ICS Network Visibility & Monitoring] | L-03  | HOCH      | sofort         |
| M-04 | Persönliche, zeitlich begrenzte Service-Konten statt geteilter Admin-Passwörter, keine Zugangsdaten in Tickets [CC4 Secure Remote Access]                                                                                                                 | L-04  | MITTEL    | 0 bis 3 Monate |
| M-05 | CRA-Meldeablauf (24 h / 72 h) mit einem angenommenen Fall einer aktiv ausgenutzten Lücke im eigenen Produkt als Übung durchspielen [CC1 ICS Incident Response]                                                                                            | L-03  | MITTEL    | 0 bis 3 Monate |

## Fragen für das nächste Jour fixe

1. Wissen wir, in wie vielen ausgelieferten Anlagen der S7-1500-Webserver aktiv ist, und wer informiert die Kunden?
2. Betreiben wir BeyondTrust oder ein vergleichbares Fernwartungs-Gateway selbst, und welche Kunden-Zugangsdaten liegen darauf?
3. Würden wir auf unseren Service-Laptops erkennen, wenn msixexec.exe ein SiemensSoftwareCenter.exe in AppData\Local\Programs startet?
4. Wer meldet bei uns innerhalb von 24 Stunden an die ENISA-Plattform, wenn eine Lücke in unserem Produkt aktiv ausgenutzt wird, und wurde das schon einmal geübt?
5. Stehen in unserem Ticket-System Passwörter für Kundenanlagen im Klartext?

## Maßnahmen dieser Woche

1. BeyondTrust-Appliances patchen (BT26-05-RS), forensisch prüfen lassen und alle dort hinterlegten Zugangsdaten für Kundenanlagen wechseln.
2. Windows-, Engineering- und Service-PCs auf ClickFix/MSI-Ausführungen und auf SiemensSoftwareCenter.exe in AppData\Local\Programs prüfen, die von msixexec.exe gestartet wurde, die drei Siemens-LoCs in Firewall und Proxy sperren und eigene Installationen auf 4.0.9.8 bringen.
3. Kundenhinweis zu ICSA-26-295-14 verschicken: S7-1500-Webserver abschalten oder auf vertrauenswürdige IPs begrenzen, nur vertrauenswürdige Trace-Dateien hochladen.
4. Die fünf CVEs aus dem SafePay-Advisory gegen eigene Firewalls, VPN-Gateways und Backup-Systeme prüfen und MFA am VPN erzwingen.
5. Ticket- und CRM-System nach Zugangsdaten im Klartext durchsuchen, sie entfernen und die betroffenen Passwörter wechseln.

### HINWEIS ZUR QUELLENLAGE

Die Meldungen L-01, L-02, L-06 und L-07 sind an CISA-Primärquellen bzw. an der Loxone-Seite (L-05) geprüft. Nicht aufgenommen: WAGO ICSA-26-293-02, weil die CISA-Seite beim Abruf einen 404-Fehler lieferte. Nicht aufgenommen, weil unbestätigt: das Opfer Passavant Energy & Environment auf der Leak-Site von Settra (nur Angaben der Täter), die Behauptungen der Gruppe „Samurai“ zu 200 GB und Miniserver-Seriennummern bei Loxone und ein neuer Meilenstein zur Maschinenverordnung (die nächste gesicherte Frist ist weiterhin der 20.01.2027). Alle Quellenlinks wurden am 23.10.2026 automatisch aufgerufen und inhaltlich geprüft. 1 Meldung(en) ohne überprüfbare Originalquelle wurden nicht aufgenommen. 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.