OT-CYBER.DE

LAGEBILD

# OT-/Cyber-Lagebild

Ausgabe 18.10.2026, 16:12 Uhr · Betreiber und Maschinenbauer in Bayern, Salzburg, Tirol und ganz DACH

| | |
|---|---|
| **Zielgruppe** | Stadtwerke, Wasser- und Energieversorger, Industrie, Maschinenbau, KRITIS |
| **Datum** | 18.10.2026 |
| **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 4 Meldungen, davon 2 mit hoher Relevanz für Betreiber in DACH.

• UPDATE: **BeyondTrust Remote Support: Zuordnung mutmaßlich zu China, Neustart und Konfigurations-Reset reichen nicht (CVE-2026-102764)**: Mandiant (Google) ordnet die Ausnutzung der mutmaßlich chinesischen, staatlich unterstützten Gruppe Armory Castle (UNC5221) zu, BeyondTrust bestätigt diese Einschätzung. Die Angreifer konnten alle Zugangsdaten abgreifen, die auf der Appliance gespeichert waren, und Dateien so verändern, dass die Änderungen Neustarts und das Zurücksetzen der Konfiguration überstehen. Eingesetzt wurden die Malware Sawfly und Bareclaw. Mandiant rät, jede verwundbare, aus dem Internet erreichbare Appliance als potenziell kompromittiert zu behandeln, bis sie überprüft ist. Unsere Einschätzung: Wer BeyondTrust für die Fernwartung nutzt, sollte alle dort hinterlegten Zugangsdaten ändern, auch die für OT-Jump-Hosts, und die Appliance auf Spuren prüfen. Quelle: https://therecord.media/beyond-trust-cyberattack-china

• **Nextcloud mit der App „Built-in CODE Server“ von Collabora: Lücke wird ausgenutzt (CVE-2026-110447, CVSS 4.0: 9,2)**: In der App richdocumentscode vor Version 26.4.303 lassen sich über proxy.php ohne Anmeldung Betriebssystembefehle einschleusen, wenn der integrierte CODE-Server gerade nicht läuft (etwa nach Neustart, Update oder Absturz). Laut BleepingComputer berichten Admins seit etwa 10.09. von Angriffen, dabei wurden PHP-Webshells abgelegt, mit denen die Angreifer nach Passwortdatenbanken und Krypto-Wallets suchten. Einzelne Nutzer berichten auch von Ransomware, BleepingComputer konnte das nicht bestätigen. Eigenständige Collabora-Server, Docker-, RPM- und DEB-Installationen sowie Nextcloud All-in-One sind laut Collabora nicht betroffen. Die App nur zu deaktivieren reicht laut Hersteller nicht. Deshalb auf 26.4.303 oder neuer aktualisieren oder die App entfernen, wenn sie nicht gebraucht wird, und den Server auf Webshells prüfen. Quellen: https://www.bleepingcomputer.com/news/security/hackers-exploit-collabora-rce-flaw-to-backdoor-nextcloud-servers/ · https://app.opencve.io/cve/CVE-2026-110447

**GESAMTBEWERTUNG**

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

# Lageübersicht

| ID | Meldung | Relevanz |
|---|---|---|
| L-01 | UPDATE: **BeyondTrust Remote Support: Zuordnung mutmaßlich zu China, Neustart und Konfigurations-Reset reichen nicht (CVE-2026-102764)**: Mandiant (Google) ordnet die Ausnutzung der mutmaßlich chinesischen, staatlich unterstützten Gruppe Armory Castle (UNC5221) zu, BeyondTrust bestätigt diese Einschätzung. Die Angreifer konnten alle Zugangsdaten abgreifen, die auf der Appliance gespeichert waren, und Dateien so verändern, dass die Änderungen Neustarts und das Zurücksetzen der Konfiguration überstehen. Eingesetzt wurden die Malware Sawfly und Bareclaw. Mandiant rät, jede verwundbare, aus dem Internet erreichbare Appliance als potenziell kompromittiert zu behandeln, bis sie überprüft ist. Unsere Einschätzung: Wer BeyondTrust für die Fernwartung nutzt, sollte alle dort hinterlegten Zugangsdaten ändern, auch die für OT-Jump-Hosts, und die Appliance auf Spuren prüfen. Quelle: https://therecord.media/beyond-trust-cyberattack-china | HOCH |

| ID | Meldung | Relevanz |
|---|---|---|
| L-02 | **Nextcloud mit der App „Built-in CODE Server“ von Collabora: Lücke wird ausgenutzt (CVE-2026-110447, CVSS 4.0: 9,2)**: In der App richdocumentscode vor Version 26.4.303 lassen sich über proxy.php ohne Anmeldung Betriebssystembefehle einschleusen, wenn der integrierte CODE-Server gerade nicht läuft (etwa nach Neustart, Update oder Absturz). Laut BleepingComputer berichten Admins seit etwa 10.09. von Angriffen, dabei wurden PHP-Webshells abgelegt, mit denen die Angreifer nach Passwortdatenbanken und Krypto-Wallets suchten. Einzelne Nutzer berichten auch von Ransomware, BleepingComputer konnte das nicht bestätigen. Eigenständige Collabora-Server, Docker-, RPM- und DEB-Installationen sowie Nextcloud All-in-One sind laut Collabora nicht betroffen. Die App nur zu deaktivieren reicht laut Hersteller nicht. Deshalb auf 26.4.303 oder neuer aktualisieren oder die App entfernen, wenn sie nicht gebraucht wird, und den Server auf Webshells prüfen. Quellen: https://www.bleepingcomputer.com/news/security/hackers-exploit-collabora-rce-flaw-to-backdoor-nextcloud-servers/ · https://app.opencve.io/cve/CVE-2026-110447 | HOCH |
| L-03 | UPDATE: **Red Lion N-Tron 700 (Industrie-Switches): sieben Lücken, Update A des Advisories ICSA-26-281-01 vom 15.10.**: Betroffen sind Firmware bis 3.11.0 und Bootloader bis 2.0.6.1. Über SNMP lassen sich ohne Anmeldung administrative Aktionen auslösen, etwa Konfiguration abrufen, Konten ändern oder Firmware einspielen (CVE-2026-33367, CVSS 4.0: 8,6). Firmware- und Bootloader-Updates laufen ohne Anmeldung und ohne Integritätsprüfung (CVE-2026-29797, 7,1). Dazu kommen werkseitige Admin-Zugangsdaten, die aktiv bleiben (CVE-2026-32645, 8,3), und schwach verschlüsselt gespeicherte Zugangsdaten (CVE-2026-28745, 9,3). Mit Update A hat die CISA die CVSS-Werte aktualisiert, die Erstfassung stammt vom 08.10. Abhilfe laut Hersteller: Firmware 3.11.1 oder neuer, SNMP-Communities setzen oder SNMP abschalten, Web-GUI sperren. Laut CISA ist keine öffentliche Ausnutzung bekannt. Quellen: https://www.cisa.gov/news-events/ics-advisories/icsa-26-281-01 · https://app.opencve.io/cve/CVE-2026-33367 | MITTEL |
| L-04 | **Spionagegruppe „Silent Lynx“ hatte russische Raffinerie Orsk im Visier und drang in die Regionalregierung Nischni Nowgorod ein**: Das berichten Forscher von Cisco Talos (Bezeichnung UAT-6275) und Recorded Future (TAG-193) in einem gemeinsamen Bericht, Reuters meldete das am 14.10., Security Affairs am 15.10. Der Einstieg lief über Spear-Phishing mit amtlich wirkenden Anhängen, verschickt teils über gekaperte Behördenkonten in Tadschikistan und Kirgisistan. Seit April 2026 nutzt die Gruppe auch die WinRAR-Lücke CVE-2025-8088. Ob der Angriff auf die Raffinerie Erfolg hatte, ist unklar; die Anlage war laut Reuters schon seit einem Drohnenangriff im August außer Betrieb. Die Forscher verorten die Gruppe wahrscheinlich in Kasachstan, gestützt auf Indizien wie Commit-Zeiten und VPN-Adressen. Unsere Einschätzung: Der Fall zeigt, dass Spionage gegen Energieanlagen über die Büro-IT beginnen kann, auch für Versorger in DACH. Quellen: https://securityaffairs.com/?p=201003 · https://www.devdiscourse.com/article/international/3992406-kazakhstan-linked-hackers-targeted-russian-refinery-spied-on-city-government-researchers-say | MITTEL |

# Meldungen im Detail

**L-01 UPDATE: **BeyondTrust Remote Support: Zuordnung mutmaßlich zu China, Neustart und Konfigurations-Reset reichen nicht (CVE-2026-102764)**: Mandiant (Google) ordnet die Ausnutzung der mutmaßlich chinesischen, staatlich unterstützten Gruppe Armory Castle (UNC5221) zu, BeyondTrust bestätigt diese Einschätzung. Die Angreifer konnten alle Zugangsdaten abgreifen, die auf der Appliance gespeichert waren, und Dateien so verändern, dass die Änderungen Neustarts und das Zurücksetzen der Konfiguration überstehen. Eingesetzt wurden die Malware Sawfly und Bareclaw. Mandiant rät, jede verwundbare, aus dem Internet erreichbare Appliance als potenziell kompromittiert zu behandeln, bis sie überprüft ist. Unsere Einschätzung: Wer BeyondTrust für die Fernwartung nutzt, sollte alle dort hinterlegten Zugangsdaten ändern, auch die für OT-Jump-Hosts, und die Appliance auf Spuren prüfen. Quelle: https://therecord.media/beyond-trust-cyberattack-china**

Relevanz: HOCH

**L-02 **Nextcloud mit der App „Built-in CODE Server“ von Collabora: Lücke wird ausgenutzt (CVE-2026-110447, CVSS 4.0: 9,2)**: In der App richdocumentscode vor Version 26.4.303 lassen sich über proxy.php ohne Anmeldung Betriebssystembefehle einschleusen, wenn der integrierte CODE-Server gerade nicht läuft (etwa nach Neustart, Update oder Absturz). Laut BleepingComputer berichten Admins seit etwa 10.09. von Angriffen, dabei wurden PHP-Webshells abgelegt, mit denen die Angreifer nach Passwortdatenbanken und Krypto-Wallets suchten. Einzelne Nutzer berichten auch von Ransomware, BleepingComputer konnte das nicht bestätigen. Eigenständige Collabora-Server, Docker-, RPM- und DEB-Installationen sowie Nextcloud All-in-One sind laut Collabora nicht betroffen. Die App nur zu deaktivieren reicht laut Hersteller nicht. Deshalb auf 26.4.303 oder neuer aktualisieren oder die App entfernen, wenn sie nicht gebraucht wird, und den Server auf Webshells prüfen. Quellen: https://www.bleepingcomputer.com/news/security/hackers-exploit-collabora-rce-flaw-to-backdoor-nextcloud-servers/ · https://app.opencve.io/cve/CVE-2026-110447**

Relevanz: HOCH

**L-03  UPDATE: **Red Lion N-Tron 700 (Industrie-Switches): sieben Lücken, Update A des Advisories ICSA-26-281-01 vom 15.10.**: Betroffen sind Firmware bis 3.11.0 und Bootloader bis 2.0.6.1. Über SNMP lassen sich ohne Anmeldung administrative Aktionen auslösen, etwa Konfiguration abrufen, Konten ändern oder Firmware einspielen (CVE-2026-33367, CVSS 4.0: 8,6). Firmware- und Bootloader-Updates laufen ohne Anmeldung und ohne Integritätsprüfung (CVE-2026-29797, 7,1). Dazu kommen werkseitige Admin-Zugangsdaten, die aktiv bleiben (CVE-2026-32645, 8,3), und schwach verschlüsselt gespeicherte Zugangsdaten (CVE-2026-28745, 9,3). Mit Update A hat die CISA die CVSS-Werte aktualisiert, die Erstfassung stammt vom 08.10. Abhilfe laut Hersteller: Firmware 3.11.1 oder neuer, SNMP-Communities setzen oder SNMP abschalten, Web-GUI sperren. Laut CISA ist keine öffentliche Ausnutzung bekannt. Quellen: https://www.cisa.gov/news-events/ics-advisories/icsa-26-281-01 · https://app.opencve.io/cve/CVE-2026-33367**

Relevanz: MITTEL

**L-04 **Spionagegruppe „Silent Lynx“ hatte russische Raffinerie Orsk im Visier und drang in die Regionalregierung Nischni Nowgorod ein**: Das berichten Forscher von Cisco Talos (Bezeichnung UAT-6275) und Recorded Future (TAG-193) in einem gemeinsamen Bericht, Reuters meldete das am 14.10., Security Affairs am 15.10. Der Einstieg lief über Spear-Phishing mit amtlich wirkenden Anhängen, verschickt teils über gekaperte Behördenkonten in Tadschikistan und Kirgisistan. Seit April 2026 nutzt die Gruppe auch die WinRAR-Lücke CVE-2025-8088. Ob der Angriff auf die Raffinerie Erfolg hatte, ist unklar; die Anlage war laut Reuters schon seit einem Drohnenangriff im August außer Betrieb. Die Forscher verorten die Gruppe wahrscheinlich in Kasachstan, gestützt auf Indizien wie Commit-Zeiten und VPN-Adressen. Unsere Einschätzung: Der Fall zeigt, dass Spionage gegen Energieanlagen über die Büro-IT beginnen kann, auch für Versorger in DACH. Quellen: https://securityaffairs.com/?p=201003 · https://www.devdiscourse.com/article/international/3992406-kazakhstan-linked-hackers-targeted-russian-refinery-spied-on-city-government-researchers-say**

Relevanz: MITTEL

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