OT-CYBER.DE

LAGEBILD

OT-/Cyber-Lagebild

Ausgabe 14.11.2026, 17:22 Uhr · Betreiber und Maschinenbauer in Bayern, Salzburg, Tirol und ganz DACH

Zielgruppe	Stadtwerke, Wasser- und Energieversorger, Industrie, Maschinenbau, KRITIS
Datum	14.11.2026
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 3 Meldungen, davon 1 mit hoher Relevanz für Betreiber in DACH.

• □ UPDATE: **Update PHP2Shell: Siemens-Netzleittechnik Spectrum Power betroffen (ICSA-26-316-01)**: CISA hat am 12.11. das Siemens-Advisory SSA-166980 zu CVE-2026-109618 (CVSS 3.1: 9,8) und CVE-2026-109619 (CVSS 3.1: 8,1) übernommen

GESAMTBEWERTUNG

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

Lageübersicht

ID	Meldung	Relevanz
L-01	□ UPDATE: **Update PHP2Shell: Siemens-Netzleittechnik Spectrum Power betroffen (ICSA-26-316-01)**: CISA hat am 12.11. das Siemens-Advisory SSA-166980 zu CVE-2026-109618 (CVSS 3.1: 9,8) und CVE-2026-109619 (CVSS 3.1: 8,1) übernommen	HOCH
L-02	**FBI-Flash zu ARTEX: KI-gestütztes Angriffsframework automatisiert Angriffe (FLASH-20261113-001)**: Das FBI hat am 13.11. eine Flash-Warnung zu ARTEX veröffentlicht	MITTEL
L-03	**Bundestag beschließt Reform des Nachrichtendienstrechts: BND darf künftig aktiv eingreifen**: Der Bundestag hat am 13.11. den Gesetzentwurf zur Reform des Nachrichtendienstrechts angenommen, in namentlicher Abstimmung mit 308 Ja-Stimmen, 190 Nein-Stimmen und 71 Enthaltungen	MITTEL

Meldungen im Detail

L-01 □ UPDATE: **Update PHP2Shell: Siemens-Netzleittechnik Spectrum Power betroffen (ICSA-26-316-01)**: CISA hat am 12.11. das Siemens-Advisory SSA-166980 zu CVE-2026-109618 (CVSS 3.1: 9,8) und CVE-2026-109619 (CVSS 3.1: 8,1) übernommen

Relevanz: HOCH

Siemens hatte SSA-166980 am 26.10. erstmals veröffentlicht. Die aktuelle Fassung listet unter anderem Produkte aus der Energietechnik: Spectrum Power 3, 4, 7 und TG, AMIS TS, Energy Engage, blueplanet 360 und Local Monitoring. Für Spectrum Power 3 und 7 nennt Siemens PHP-Patches von Red Hat, für Spectrum Power TG und Energy Engage V3.1SP1 ein PHP-Update. Für Spectrum Power 4, AMIS TS und blueplanet 360 gibt es noch keinen Fix, für Energy Engage V2.0SP9 ist keiner geplant. Eine Ausnutzung erwähnt das Advisory nicht. Unsere Einschätzung: Spectrum Power wird in Netzleitstellen eingesetzt. Netzbetreiber und Stadtwerke mit Siemens-Netzleittechnik sollten ihre Versionen prüfen und den Netzzugriff auf die betroffenen Web- und Monitoring-Komponenten einschränken, solange kein Fix da ist (CC5 Risk-Based Vulnerability Management der SANS Five ICS Critical Controls).

Quelle: https://www.cisa.gov/news-events/ics-advisories/icsa-26-316-01

Quelle: https://ot-cyber.de/blog/vorfall-lagebild-php2shell-folgen-fuer-ot-anlagen-und-firewalls.html

Quelle: https://ot-cyber.de/ot-lage/2026-11-11.html

L-02 **FBI-Flash zu ARTEX: KI-gestütztes Angriffsframework automatisiert Angriffe (FLASH-20261113-001)**: Das FBI hat am 13.11. eine Flash-Warnung zu ARTEX veröffentlicht

Relevanz: MITTEL

ARTEX ist laut FBI ein Open-Source-Framework, das Sprachmodelle anbindet und mehrere Angriffsphasen automatisiert, von der Aufklärung bis zur Datenausleitung. Verschiedene Threat Actors nutzen es laut FBI für Kampagnen in vielen Branchen, darunter Energie und Fertigung. Manche Angriffe kamen in unter drei Stunden bis zu privilegiertem Zugriff. Laut FBI fanden Forscher Anfang November über 1.600 öffentlich erreichbare ARTEX-Konsolen. Besonders im Visier sind laut Flash Systeme, die weniger Aufmerksamkeit bekommen: Partner- und Lieferantenportale, Legacy-Dienste und Anbindungen von Drittanbietern. Unter den beobachteten Techniken nennt das FBI auch gestohlene VPN-Konfigurationen und Zugangsdaten. ICS- oder OT-Systeme nennt das FBI nicht ausdrücklich. Unsere Einschätzung: Bei Versorgern und Maschinenbauern gehören Fernwartungs- und Dienstleisterzugänge zu genau diesen Randsystemen. Wir empfehlen, jeden VPN- und Fernwartungszugang im Asset-Inventar zu erfassen und mit eigener Anmeldung pro Dienstleister abzusichern (CC4 Secure Remote Access).

Quelle: https://www.ic3.gov/CSA/2026/261113.pdf

L-03 **Bundestag beschließt Reform des Nachrichtendienstrechts: BND darf künftig aktiv eingreifen**: Der Bundestag hat am 13.11. den Gesetzentwurf zur Reform des Nachrichtendienstrechts angenommen, in namentlicher Abstimmung mit 308 Ja-Stimmen, 190 Nein-Stimmen und 71 Enthaltungen

Relevanz: MITTEL

Die Reform sieht laut Bundestag aktive Maßnahmen vor, zum Beispiel das Abschalten der Server staatlicher Hackergruppen. In der Debatte wurde als Beispiel eine staatliche Hackergruppe genannt, die in Deutschland Daten von KRITIS-Firmen abzieht. Die Vorabkontrolle von Anordnungen geht an den Unabhängigen Kontrollrat. Unsere Einschätzung: Die neuen Befugnisse richten sich gegen Angreifer und ihre Infrastruktur. Erkennen, Melden und Wiederanlauf nach einem Angriff bleiben Aufgabe des Betreibers (CC1 ICS Incident Response).

Quelle: https://www.bundestag.de/dokumente/textarchiv/2026/kw46-de-nachrichtendienste-1231530

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