

L A G E B I L D

OT-/Cyber-Lagebild

Ausgabe 24.10.2026, 16:29 Uhr · Betreiber und Maschinenbauer in Bayern, Salzburg, Tirol und ganz DACH

Zielgruppe	Stadtwerke, Wasser- und Energieversorger, Industrie, Maschinenbau, KRITIS
Datum	24.10.2026
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 3 mit hoher Relevanz für Betreiber in DACH.

- ****PHP2Shell:** Amazon sieht breite Ausnutzungsversuche, Rockwell prüft sein Portfolio (23.10.)****:** Laut Amazon (CJ Moses, AWS) gibt es inzwischen „broad exploitation attempts in the wild“ gegen PHP2Shell. Die Angriffe begannen nach Amazon-Angaben vier Tage vor den Patches, die unterschiedlichen Payloads deuten auf mehrere Threat Actors hin. Ob Angriffe erfolgreich waren, ist offen. Rockwell Automation hat am 23.10. das Advisory SD1802 (kritisch) veröffentlicht. Bestätigt betroffene Rockwell-Produkte gibt es laut Advisory derzeit nicht, Rockwell prüft das Portfolio noch. Betroffen sind PHP-Versionen vor 8.2.35, 8.3.36, 8.4.27 und 8.5.12. Censys zählt in Deutschland rund 4,2 Mio. PHP-Dienste mit einer als verwundbar geltenden Versionsnummer. Das ist eine Schätzung allein nach Versionsnummer, zurückportierte Patches der Linux-Distributionen erkennt sie nicht. Unsere Einschätzung: Webbasierte HMI, Engineering-Portale und Gateways mit PHP gehören jetzt ins Asset-Inventar, und die Rockwell-Seite sollte man in den nächsten Tagen im Blick behalten. Quelle: <https://www.bleepingcomputer.com/news/security/php-shares-mitigation-for-new-and-unpatched-rce-vulnerability/> und <https://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.SD1802.html> und <https://www.heise.de/news/php2shell-Millionen-PHP-Dienste-in-Deutschland-verwundbar-11498464.html>
- **□ UPDATE: **PHP2Shell:** Siemens RUGGEDCOM APE1808 betroffen, Patch nur über den Siemens-Support (SSA-566512, 23.10.)****:** Siemens hat am 23.10. ein eigenes Advisory für die RUGGEDCOM APE1808 mit Palo Alto PAN-OS veröffentlicht. Betroffen sind alle Versionen der PAN-OS-Zweige 10.2, 11.1, 11.2, 12.1 und 12.2. Es geht um CVE-2026-109618 (CVSS 3.1: 9,8, CVSS 4.0: 9,2) und CVE-2026-109619 (CVSS 3.1: 8,1). Eine Fix-Version nennt das Advisory nicht, Informationen zu Patches gibt es über den Siemens-Support. Bis dahin verweist Siemens auf die Workarounds von Palo Alto. Siemens beschreibt die APE1808 als Application-Hosting-Plattform in Versorger-Qualität („utility-grade“) für raue Industrieumgebungen. Unsere Einschätzung: Energieversorger und Stadtwerke, die die APE1808 einsetzen, sollten den Support jetzt kontaktieren. Siemens-Software wie Opcenter Connect MOM, Opcenter Execution Core und Opcenter X ist laut dem separaten Advisory SSA-566435 nicht betroffen. Quelle: <https://cert-portal.siemens.com/productcert/html/ssa-566512.html> und <https://cert-portal.siemens.com/productcert/html/ssa-566435.html> (Erstmeldung am 22.10.2026: <https://ot-cyber.de/ot-lage/2026-10-22.html>)
- ****PHP2Shell bei Cisco:** Fix für Industrie-Funk URWB erst im Februar 2027 (23.10.)****:** Laut Cisco-Advisory (Stand 23.10.) sind unter anderem Ultra-Reliable Wireless Backhaul (URWB), Expressway und Expressway Select bestätigt betroffen, weitere Produkte prüft Cisco noch. Für URWB ist der Fix mit Version 27.1.1 für Februar 2027 angekündigt, bis dahin gibt es einen Workaround. Cisco stuft URWB mit CVSS 6,6 ein, weil ein Angreifer Admin-Rechte braucht. Für Expressway ist der Fix 15.5.21 angekündigt, ein Termin steht noch nicht fest. Unsere Einschätzung: Wer URWB einsetzt, sollte die Geräte im Asset-Inventar erfassen und den Management-Zugang strikt segmentieren. Quelle: <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-php-october26-Jj384Daq> und <https://www.heise.de/news/Cisco-stopft-diverse-teils-kritische-Sicherheitsluecken-11497857.html>

GESAMTBEWERTUNG

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

Lageübersicht

ID	Meldung	Relevanz
L-01	<p>**PHP2Shell: Amazon sieht breite Ausnutzungsversuche, Rockwell prüft sein Portfolio (23.10.)**: Laut Amazon (CJ Moses, AWS) gibt es inzwischen „broad exploitation attempts in the wild“ gegen PHP2Shell. Die Angriffe begannen nach Amazon-Angaben vier Tage vor den Patches, die unterschiedlichen Payloads deuten auf mehrere Threat Actors hin. Ob Angriffe erfolgreich waren, ist offen. Rockwell Automation hat am 23.10. das Advisory SD1802 (kritisch) veröffentlicht. Bestätigt betroffene Rockwell-Produkte gibt es laut Advisory derzeit nicht, Rockwell prüft das Portfolio noch. Betroffen sind PHP-Versionen vor 8.2.35, 8.3.36, 8.4.27 und 8.5.12. Censys zählt in Deutschland rund 4,2 Mio. PHP-Dienste mit einer als verwundbar geltenden Versionsnummer. Das ist eine Schätzung allein nach Versionsnummer, zurückportierte Patches der Linux-Distributionen erkennt sie nicht. Unsere Einschätzung: Webbasierte HMI, Engineering-Portale und Gateways mit PHP gehören jetzt ins Asset-Inventar, und die Rockwell-Seite sollte man in den nächsten Tagen im Blick behalten. Quelle: https://www.bleepingcomputer.com/news/security/php-shares-mitigation-for-new-and-unpatched-rce-vulnerability/ und https://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.SD1802.html und https://www.heise.de/news/php2shell-Millionen-PHP-Dienste-in-Deutschland-verwundbar-11498464.html</p>	HOCH
L-02	<p>**CISA nimmt Collabora Online und Arista VeloCloud Orchestrator in den KEV-Katalog auf (23.10.)**: CISA hat am 23.10. zwei aktiv ausgenutzte Schwachstellen in den Known-Exploited-Vulnerabilities-Katalog aufgenommen. CVE-2026-110447 ist eine OS Command Injection im eingebauten CODE-Server von Collabora Online. CVE-2026-114625 ist eine SQL-Injection im Arista VeloCloud Orchestrator. Unsere Einschätzung: Wer Collabora Online oder den VeloCloud Orchestrator selbst betreibt, sollte Updates und Herstellerhinweise mit Vorrang umsetzen, weil die Lücken laut CISA bereits ausgenutzt werden. Quelle: https://www.cisa.gov/news-events/alerts/2026/10/23/cisa-adds-one-known-exploited-vulnerability-catalog-0 und https://www.cisa.gov/news-events/alerts/2026/10/23/cisa-adds-one-known-exploited-vulnerability-catalog</p>	MITTEL
L-03	<p>□ UPDATE: **PHP2Shell: Siemens RUGGEDCOM APE1808 betroffen, Patch nur über den Siemens-Support (SSA-566512, 23.10.)**: Siemens hat am 23.10. ein eigenes Advisory für die RUGGEDCOM APE1808 mit Palo Alto PAN-OS veröffentlicht. Betroffen sind alle Versionen der PAN-OS-Zweige 10.2, 11.1, 11.2, 12.1 und 12.2. Es geht um CVE-2026-109618 (CVSS 3.1: 9,8, CVSS 4.0: 9,2) und CVE-2026-109619 (CVSS 3.1: 8,1). Eine Fix-Version nennt das Advisory nicht, Informationen zu Patches gibt es über den Siemens-Support. Bis dahin verweist Siemens auf die Workarounds von Palo Alto. Siemens beschreibt die APE1808 als Application-Hosting-Plattform in Versorger-Qualität („utility-grade“) für raue Industrieumgebungen. Unsere Einschätzung: Energieversorger und Stadtwerke, die die APE1808 einsetzen, sollten den Support jetzt kontaktieren. Siemens-Software wie Opcenter Connect MOM, Opcenter Execution Core und Opcenter X ist laut dem separaten Advisory SSA-566435 nicht betroffen. Quelle: https://cert-portal.siemens.com/productcert/html/ssa-566512.html und https://cert-portal.siemens.com/productcert/html/ssa-566435.html (Erstmeldung am 22.10.2026: https://ot-cyber.de/ot-lage/2026-10-22.html)</p>	HOCH

ID	Meldung	Relevanz
L-04	<p>**PHP2Shell bei Cisco: Fix für Industrie-Funk URWB erst im Februar 2027 (23.10.)**: Laut Cisco-Advisory (Stand 23.10.) sind unter anderem Ultra-Reliable Wireless Backhaul (URWB), Expressway und Expressway Select bestätigt betroffen, weitere Produkte prüft Cisco noch. Für URWB ist der Fix mit Version 27.1.1 für Februar 2027 angekündigt, bis dahin gibt es einen Workaround. Cisco stuft URWB mit CVSS 6,6 ein, weil ein Angreifer Admin-Rechte braucht. Für Expressway ist der Fix 15.5.21 angekündigt, ein Termin steht noch nicht fest. Unsere Einschätzung: Wer URWB einsetzt, sollte die Geräte im Asset-Inventar erfassen und den Management-Zugang strikt segmentieren. Quelle: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-php-october26-jj384Daq und https://www.heise.de/news/Cisco-stopft-diverse-teils-kritische-Sicherheitsluecke-n-11497857.html</p>	HOCH
L-05	<p>**Cisco Cyber Vision (OT-Monitoring) mit kritischen Snort-3-Lücken (21.10.)**: Im Snort-3-Hardening-Release vom Oktober 2026 schließt Cisco vier Lücken, zwei davon kritisch mit CVSS 9,0 (CVE-2026-20236 und CVE-2026-20043), dazu CVE-2026-20291 (7,8) und CVE-2026-20356 (7,5). Betroffen ist auch Cyber Vision, die OT-Angriffserkennung von Cisco: Versionen vor 5.6 sind verwundbar, behoben ist es ab 5.6.0, bei Open Source Snort 3 mit dem aktuellen Release. Workarounds gibt es laut Cisco nicht. Unsere Einschätzung: Fällt die Sensorik aus, sieht man in der Angriffserkennung (SzA) nichts mehr. Quelle: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-snort3-ybgmhTQe und https://cyber.gc.ca/en/alerts-advisories/cisco-security-advisory-av26-1073</p>	MITTEL
L-06	<p>**Edge-Geräte im Visier: Threat Actor „k0t“ versucht u. a. CVE-2026-0257 auszunutzen (Bericht vom 21.10.)**: Group-IB und NyxLab beschreiben einen Threat Actor namens „k0t“, der FortiGate-, FortiWeb- und GlobalProtect-Geräte angegriffen hat. Group-IB spricht von über 70.000 offengelegten Zugangsdaten aus Netzwerkgeräten und LDAP-Dumps. Laut Group-IB versuchte k0t, CVE-2026-0257 und die FortiWeb-Lücke CVE-2025-64446 auszunutzen, dazu kam Brute-Force. Viele der FortiGate-Einbrüche stammen aus Februar bis Juni 2026. Europa gehört zu den Zielregionen. Unsere Einschätzung: Wer VPN-Zugänge über diese Geräte betreibt, sollte Zugangsdaten tauschen und MFA prüfen. Quelle: https://thehackernews.com/2026/10/hackers-breach-enterprise-firewalls-and.html und https://www.group-ib.com/blog/stray-cat-network-edge/</p>	MITTEL
L-07	<p>**ESET: UAC-0099 und Sandworm, neue Backdoor mit C2 im Mesh-Netz**: Bei einem ukrainischen Getreidelogistik-Unternehmen verschaffte sich UAC-0099 im Juli 2025 per Spear-Phishing Zugang und übergab an Sandworm, das im September 2025 SDelete als Wiper per Gruppenrichtlinie verteilte. Dazu kam die bisher unbekannte Backdoor MythicRatatoskr, deren C2 im Yggdrasil-Mesh-Netz liegt. Unsere Einschätzung: Verbindungen ins Yggdrasil-Netz sind ein lohnender Ansatz für Threat Hunting bei KRITIS-Betreibern und in der Logistik. Quelle: https://thehackernews.com/2026/10/russian-linked-hackers-used-new-mesh.html und https://www.welivesecurity.com/en/eset-research/mythicratatoskr-yggdrasil-enabled-backdoor-deployed-uac0099-sandworm-collaboration/</p>	MITTEL

Meldungen im Detail

L-01 **PHP2Shell: Amazon sieht breite Ausnutzungsversuche, Rockwell prüft sein Portfolio (23.10.):** Laut Amazon (CJ Moses, AWS) gibt es inzwischen „broad exploitation attempts in the wild“ gegen PHP2Shell. Die Angriffe begannen nach Amazon-Angaben vier Tage vor den Patches, die unterschiedlichen Payloads deuten auf mehrere Threat Actors hin. Ob Angriffe erfolgreich waren, ist offen. Rockwell Automation hat am 23.10. das Advisory SD1802 (kritisch) veröffentlicht. Bestätigt betroffene Rockwell-Produkte gibt es laut Advisory derzeit nicht, Rockwell prüft das Portfolio noch. Betroffen sind PHP-Versionen vor 8.2.35, 8.3.36, 8.4.27 und 8.5.12. Censys zählt in Deutschland rund 4,2 Mio. PHP-Dienste mit einer als verwundbar geltenden Versionsnummer. Das ist eine Schätzung allein nach Versionsnummer, zurückportierte Patches der Linux-Distributionen erkennt sie nicht. Unsere Einschätzung: Webbasierte HMI, Engineering-Portale und Gateways mit PHP gehören jetzt ins Asset-Inventar, und die Rockwell-Seite sollte man in den nächsten Tagen im Blick behalten. Quelle: <https://www.bleepingcomputer.com/news/security/php-shares-mitigation-for-new-and-unpatched-rce-vulnerability/> und <https://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.SD1802.html> und <https://www.heise.de/news/php2shell-Millionen-PHP-Dienste-in-Deutschland-verwundbar-11498464.html>

Relevanz: **HOCH**

L-02 **CISA nimmt Collabora Online und Arista VeloCloud Orchestrator in den KEV-Katalog auf (23.10.):** CISA hat am 23.10. zwei aktiv ausgenutzte Schwachstellen in den Known-Exploited-Vulnerabilities-Katalog aufgenommen. CVE-2026-110447 ist eine OS Command Injection im eingebauten CODE-Server von Collabora Online. CVE-2026-114625 ist eine SQL-Injection im Arista VeloCloud Orchestrator. Unsere Einschätzung: Wer Collabora Online oder den VeloCloud Orchestrator selbst betreibt, sollte Updates und Herstellerhinweise mit Vorrang umsetzen, weil die Lücken laut CISA bereits ausgenutzt werden. Quelle: <https://www.cisa.gov/news-events/alerts/2026/10/23/cisa-adds-one-known-exploited-vulnerability-catalog-0> und <https://www.cisa.gov/news-events/alerts/2026/10/23/cisa-adds-one-known-exploited-vulnerability-catalog>

Relevanz: **MITTEL**

L-03 □ UPDATE: **PHP2Shell: Siemens RUGGEDCOM APE1808 betroffen, Patch nur über den Siemens-Support (SSA-566512, 23.10.):** Siemens hat am 23.10. ein eigenes Advisory für die RUGGEDCOM APE1808 mit Palo Alto PAN-OS veröffentlicht. Betroffen sind alle Versionen der PAN-OS-Zweige 10.2, 11.1, 11.2, 12.1 und 12.2. Es geht um CVE-2026-109618 (CVSS 3.1: 9,8, CVSS 4.0: 9,2) und CVE-2026-109619 (CVSS 3.1: 8,1). Eine Fix-Version nennt das Advisory nicht, Informationen zu Patches gibt es über den Siemens-Support. Bis dahin verweist Siemens auf die Workarounds von Palo Alto. Siemens beschreibt die APE1808 als Application-Hosting-Plattform in Versorger-Qualität („utility-grade“) für raue Industrieumgebungen. Unsere Einschätzung: Energieversorger und Stadtwerke, die die APE1808 einsetzen, sollten den Support jetzt kontaktieren. Siemens-Software wie Opcenter Connect MOM, Opcenter Execution Core und Opcenter X ist laut dem separaten Advisory SSA-566435 nicht betroffen. Quelle: <https://cert-portal.siemens.com/productcert/html/ssa-566512.html> und <https://cert-portal.siemens.com/productcert/html/ssa-566435.html> (Erstmeldung am 22.10.2026: <https://ot-cyber.de/ot-lage/2026-10-22.html>)

Relevanz: **HOCH**

L-04 **PHP2Shell bei Cisco: Fix für Industrie-Funk URWB erst im Februar 2027 (23.10.):** Laut Cisco-Advisory (Stand 23.10.) sind unter anderem Ultra-Reliable Wireless Backhaul (URWB), Expressway und Expressway Select bestätigt betroffen, weitere Produkte prüft Cisco noch. Für URWB ist der Fix mit Version 27.1.1 für Februar 2027 angekündigt, bis dahin gibt es einen Workaround. Cisco stuft URWB mit CVSS 6,6 ein, weil ein Angreifer Admin-Rechte braucht. Für Expressway ist der Fix 15.5.21 angekündigt, ein Termin steht noch nicht fest. Unsere Einschätzung: Wer URWB einsetzt, sollte die Geräte im Asset-Inventar erfassen und den Management-Zugang strikt segmentieren. Quelle: <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-php-october26-Jj384Daq> und <https://www.heise.de/news/Cisco-stopft-diverse-teils-kritische-Sicherheitsluecken-11497857.html>

Relevanz: **HOCH**

L-05 **Cisco Cyber Vision (OT-Monitoring) mit kritischen Snort-3-Lücken (21.10.):** Im Snort-3-Hardening-Release vom Oktober 2026 schließt Cisco vier Lücken, zwei davon kritisch mit CVSS 9,0 (CVE-2026-20236 und CVE-2026-20043), dazu CVE-2026-20291 (7,8) und CVE-2026-20356 (7,5). Betroffen ist auch Cyber Vision, die OT-Angriffserkennung von Cisco: Versionen vor 5.6 sind verwundbar, behoben ist es ab 5.6.0, bei Open Source Snort 3 mit dem aktuellen Release. Workarounds gibt es laut Cisco nicht. Unsere Einschätzung: Fällt die Sensorik aus, sieht man in der Angriffserkennung (SzA) nichts mehr. Quelle: <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-snort3-ybgmhTQe> und <https://cyber.gc.ca/en/alerts-advisories/cisco-security-advisory-av26-1073>

Relevanz: MITTEL

L-06 **Edge-Geräte im Visier: Threat Actor „k0t“ versucht u. a. CVE-2026-0257 auszunutzen (Bericht vom 21.10.):** Group-IB und NyxLab beschreiben einen Threat Actor namens „k0t“, der FortiGate-, FortiWeb- und GlobalProtect-Geräte angegriffen hat. Group-IB spricht von über 70.000 offengelegten Zugangsdaten aus Netzwerkgeräten und LDAP-Dumps. Laut Group-IB versuchte k0t, CVE-2026-0257 und die FortiWeb-Lücke CVE-2025-64446 auszunutzen, dazu kam Brute-Force. Viele der FortiGate-Einbrüche stammen aus Februar bis Juni 2026. Europa gehört zu den Zielregionen. Unsere Einschätzung: Wer VPN-Zugänge über diese Geräte betreibt, sollte Zugangsdaten tauschen und MFA prüfen. Quelle: <https://thehackernews.com/2026/10/hackers-breach-enterprise-firewalls-and.html> und <https://www.group-ib.com/blog/stray-cat-network-edge/>

Relevanz: MITTEL

L-07 **ESET: UAC-0099 und Sandworm, neue Backdoor mit C2 im Mesh-Netz:** Bei einem ukrainischen Getreidelogistik-Unternehmen verschaffte sich UAC-0099 im Juli 2025 per Spear-Phishing Zugang und übergab an Sandworm, das im September 2025 SDelete als Wiper per Gruppenrichtlinie verteilte. Dazu kam die bisher unbekannte Backdoor MythicRatatoskr, deren C2 im Yggdrasil-Mesh-Netz liegt. Unsere Einschätzung: Verbindungen ins Yggdrasil-Netz sind ein lohnender Ansatz für Threat Hunting bei KRITIS-Betreibern und in der Logistik. Quelle: <https://thehackernews.com/2026/10/russian-linked-hackers-use-d-new-mesh.html> und <https://www.welivesecurity.com/en/eset-research/mythicratatoskr-yggdrasil-enabled-backdoor-deployed-uac0099-sandworm-collaboration/>

Relevanz: MITTEL