

WOCHENBERICHT

OT-/Cyber-Lagebild Gesamt

Ausgabe KW 44/2026 · Gesamt – alle OT-Branchen in DACH

Zielgruppe	Betreiber von Anlagen und Maschinen, KRITIS, Industrie in DACH
Berichtszeitraum	23.10.2026–30.10.2026
Version	1.0
Datum	30.10.2026
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

Die KW 44 stand im Zeichen von PHP2Shell (CVE-2026-109618/-109619). Die CISA hat beide Lücken am 26.10. als aktiv ausgenutzt in den KEV-Katalog aufgenommen. Palo Alto meldet Angriffe auf das Management-Interface von PAN-OS, die Hotfixes sind inzwischen verfügbar. Mehrere OT-Hersteller haben betroffene Produkte bestätigt, darunter Siemens (RUGGEDCOM APE1808), Schneider Electric, B&R APROL, Belden NetModule (ohne Patch) und HMS Netbiter. Daneben nutzen Angreifer eine Zero-Day-Lücke in Cisco ASA/FTD aus, um SSL-VPN-Geräte abstürzen zu lassen, also genau den Remote Access, über den viele Betreiber ihre Fernwartung abwickeln. Für die verbreiteten S7-1500- und ET-200SP-CPU's gibt es zu acht Webserver-Lücken weiterhin keinen Fix.

Auf der Bedrohungsseite beschreibt Bloomberg (27.10.), wie russlandnahe Hacktivist*innen über schlecht gesicherte HMIs in NATO-Staaten physische Schäden verursachen, etwa geplatzte Rohre, verdorbene Lebensmittel und Brände. In DACH bestätigte das Baukonsortium des Fehmarnbelt-Tunnels einen Ransomware-Angriff mit zeitweisem Baustopp. Neue offizielle Warnungen von BSI, CERT.at oder BACS mit OT-Bezug habe ich für diese Woche nicht gefunden. Die Lage ist erhöht. Vorrang haben Edge-Geräte mit Weboberfläche (Firewalls, VPN-Gateways, Fernwirk-Router) und alles, was an HMIs aus dem Internet erreichbar ist.

GESAMTBEWERTUNG

Die Lage ist erhöht, weil die aktiv ausgenutzten Lücken in PHP2Shell und Cisco ASA direkt Edge-Geräte und Remote Access in OT-Umgebungen treffen. Vorrang hat diese Woche, Management-Oberflächen und VPN-Zugänge zu patchen oder abzuschotten.

Trends

- Angreifer nutzen bevorzugt Edge-Geräte (Firewalls, VPN-Gateways, Router mit Weboberfläche), deshalb werden Lücken in Basiskomponenten wie PHP sofort zum OT-Thema.
- Hacktivist*innen mit Nähe zu Russland verursachen zunehmend physische Schäden, und zwar mit einfachen Mitteln über offene HMIs statt mit Zero-Days.
- Bei OT-Produkten dauert es oft lange bis zum Fix: S7-1500, NetModule und ältere ICONICS-Versionen bleiben vorerst nur über Mitigationen geschützt.
- Ransomware-Gruppen veröffentlichen gehäuft Energiehändler, Engineering-Dienstleister und Zulieferer auf ihren Leak-Sites, dort liegt oft OT-Dokumentation.

Lageübersicht

ID	Meldung	Relevanz	Quelle
L-01	PHP2Shell (CVE-2026-109618/-109619): im KEV-Katalog, Angriffe auf PAN-OS, OT-Hersteller bestätigen Betroffenheit	KRITISCH	CISA, Palo Alto Networks, SecurityWeek, Siemens ProductCERT, 26.10.
L-02	Cisco Secure Firewall ASA/FTD: Zero-Day lässt SSL-VPN-Geräte neu starten (CVE-2026-76418, CVSS 8,6)	HOCH	Cisco PSIRT, 28.10.

ID	Meldung	Relevanz	Quelle
L-03	Siemens SIMATIC S7-1500, ET 200SP und Software Controller: acht Webserver-Lücken, für viele Produkte kein Fix (ICSA-26-295-14)	HOCH	CISA / Siemens, 22.10.
L-04	Mitsubishi Electric ICONICS GENESIS64 und MC Works64: Anmeldung umgehbar, für Altprodukte kein Fix (ICSA-26-300-02)	HOCH	CISA, 27.10.
L-05	Fehmarnbelt-Tunnel: Baukonsortium FLC bestätigt Cyberangriff, Gruppe „Barracuda“ bietet 2,44 TB Daten an	MITTEL	heise online, 29.10.
L-06	WatchGuard Firewall OS: 18 Advisories, mehrere kritische Lücken ohne Anmeldung (u. a. CVE-2026-93866)	MITTEL	SecurityOnline (Hersteller-PSIRT nicht direkt geprüft), 27.10.

Exponierte OT-Systeme (Shodan)

Exponierte OT-Systeme (Shodan, Stand 30.10.2026):

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	148182	DNP3: 34267, OMRON FINS: 26328, ProConOS: 17131, Siemens S7: 7931, OPC UA: 5265
Österreich	4928	HMI/VNC: 1088, DNP3: 1006, Niagara Fox: 482, Siemens S7: 386, OPC UA: 161
Bayern (München)	1526	OMRON FINS: 837, HMI/VNC: 202, DNP3: 184, Siemens S7: 33, OPC UA: 16
Salzburg	30	HMI/VNC: 9, BACnet: 5, Niagara Fox: 5, Siemens S7: 2, OPC UA: 1
Tirol (Innsbruck)	48	HMI/VNC: 14, DNP3: 8, Niagara Fox: 7, Siemens S7: 2, OPC UA: 2

Meldungen im Detail

L-01 PHP2Shell (CVE-2026-109618/-109619): im KEV-Katalog, Angriffe auf PAN-OS, OT-Hersteller bestätigen Betroffenheit

KRITISCH CISA, Palo Alto Networks, SecurityWeek, Siemens ProductCERT, 26.10.

Was ist neu: Die CISA hat beide CVEs am 26.10. in den KEV-Katalog aufgenommen. Palo Alto meldet mit Stand 29.10. Angriffe auf erreichbare PAN-OS-Management-Interfaces (Status ATTACKED), die Hotfixes für die Zweige 10.2 bis 12.2 sind veröffentlicht. Betroffene Produkte bestätigen laut SecurityWeek unter anderem Siemens RUGGEDCOM APE1808 (Fix nur über Support), Schneider EcoStruxure Security Expert und Control Engineering, B&R APROL bis R 4.4-65, HMS Netbiter und Belden NetModule NRSW (kein Patch, Webinterface abschalten). Moxa meldet keine betroffenen Produkte, Rockwell prüft noch.

Bedeutung: PHP steckt in vielen Weboberflächen von Edge-Geräten, Gateways und Leittechnik-Komponenten. Bei Stadtwerken und Industriebetrieben sitzen genau diese Geräte zwischen IT, Internet und OT. Wer ein Management-Interface aus dem Internet erreicht, kann Code ausführen.

Empfehlung: Alle PHP-basierten Weboberflächen im Asset-Inventar markieren, verfügbare Patches einspielen und den Management-Zugang nur noch über einen Jump Host erlauben (CC2 Defensible Architecture, CC5 Risk-Based Vulnerability Management). Bei NetModule-Routern ohne Patch das Webinterface abschalten.

Quelle:

<https://www.cisa.gov/news-events/alerts/2026/10/26/cisa-adds-two-known-exploited-vulnerabilities-catalog> ✓
geprüft

L-02 Cisco Secure Firewall ASA/FTD: Zero-Day lässt SSL-VPN-Geräte neu starten (CVE-2026-76418, CVSS 8,6)

HOCH Cisco PSIRT, 28.10.

Was ist neu: Ohne Anmeldung kann ein Angreifer mit einer präparierten Anfrage einen Neustart der Firewall auslösen. Das klappt nur, wenn SSL-VPN aktiv und in einer Tunnel-Gruppe, auch in DefaultWEBVPNGroup, eine sekundäre Authentifizierung eingerichtet ist. Cisco bestätigt die Ausnutzung und nennt Fix-Versionen von ASA 9.16.4.104 bis 9.24.1.27 sowie FTD 7.0.11 bis 10.1.1. Einen echten Workaround gibt es nicht, nur Mitigationen.

Bedeutung: Bei einem Neustart fällt der Remote Access aus, auch für Bereitschaft und Dienstleister im Störfall. Wer die Fernwartung über ASA abwickelt, verliert im Angriffsfall den Zugriff von außen.

Empfehlung: ASA/FTD auf die genannten Fix-Versionen bringen und prüfen, ob die Konfiguration mit sekundärer Authentifizierung betroffen ist (CC4 Secure Remote Access). Für den Ausfall des VPN einen zweiten Zugangsweg im Incident-Response-Plan festlegen (CC1).

Quelle: <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-tunnel-dos-s6mgkb75> ✓ geprüft

L-03 Siemens SIMATIC S7-1500, ET 200SP und Software Controller: acht Webserver-Lücken, für viele Produkte kein Fix (ICSA-26-295-14)

HOCH CISA / Siemens, 22.10.

Was ist neu: CVE-2026-63350 bis -63357 betreffen über 150 Varianten in allen Versionen, CVSS v3 bis 9,6. Ein Angreifer muss einen Nutzer mit dem Recht „Read diagnostics“ dazu bringen, eine präparierte Trace-Datei zu importieren. Danach kann er im Browser des Nutzers Aktionen auf der SPS mit dessen Rechten ausführen. Siemens bereitet Fixes vor, für viele Produkte gilt noch „Currently no fix is available“.

Bedeutung: S7-1500 und ET 200SP stecken in fast jeder Anlage in DACH, von der Wasserversorgung bis zur Fertigung. Der Angriffsweg läuft über Social Engineering beim Instandhalter, deshalb hilft eine Firewall allein nicht.

Empfehlung: Den SPS-Webserver dort abschalten, wo er nicht gebraucht wird, und die Ports 80/443 auf Engineering-Stationen beschränken (CC2). Instandhaltung und Dienstleister anweisen, nur Trace-Dateien aus geprüfter Quelle zu importieren.

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

L-04 Mitsubishi Electric ICONICS GENESIS64 und MC Works64: Anmeldung umgehbar, für Altprodukte kein Fix (ICSA-26-300-02)

HOCH CISA, 27.10.

Was ist neu: Die Passwort-Wiederherstellung arbeitet mit einer festen Challenge-Response, die für alle Benutzer gleich ist. Damit lässt sich das System aus der Ferne entsperren (CVE-2026-16436, CVSS v4 9,2). Dazu kommen eine Rechteauserweiterung (CVE-2026-16438) und die libwebp-Lücke CVE-2023-4863. Für MC Works64, GENESIS32 und BizViz plant Mitsubishi keinen Fix.

Bedeutung: GENESIS64 ist in der Wasser-, Energie- und Gebäudeleittechnik als SCADA/HMI verbreitet. Für Altinstallationen ohne Fix ist eine Migration nötig, die Budget und Vorlauf braucht.

Empfehlung: Alle ICONICS-Installationen mit Version ins Asset-Inventar aufnehmen (CC5). Altsysteme vom Remote Access trennen und die Migration einplanen, bis dahin die von der CISA beschriebene Mitigation umsetzen.

Quelle: <https://www.cisa.gov/news-events/ics-advisories/icsa-26-300-02> ✓ geprüft

L-05 Fehmarnbelt-Tunnel: Baukonsortium FLC bestätigt Cyberangriff, Gruppe „Barracuda“ bietet 2,44 TB Daten an

MITTEL heise online, 29.10.

Was ist neu: Femern Link Contractors hat einen Cyberangriff bestätigt, der am 11.10. bemerkt wurde. Teile der Bauarbeiten standen zeitweise still. Laut eigener Angabe hatten die Täter seit dem 17.09. Zugriff, umgingen das EDR und verschlüsselten alle VMs im vCenter. Diese Angaben stammen nur von den Tätern und sind nicht bestätigt.

Bedeutung: Ein großes deutsch-dänisches Infrastrukturprojekt musste den Betrieb unterbrechen, obwohl die Täter laut Bericht keine OT angegriffen haben. Das zeigt, wie stark der Betrieb von der IT-Virtualisierung abhängt. Unentdeckt blieben die Täter laut eigener Aussage rund drei Wochen.

Empfehlung: Die vCenter-Verwaltung vom Büronetz trennen, den Admin-Zugang mit MFA absichern und Backups offline halten (CC2). Den Wiederanlauf ohne vCenter einmal durchspielen (CC1).

Quelle: <https://www.heise.de/news/Cyberangriff-auf-Fehmarnbelt-Tunnel-Gesellschaft-Cybergang-meldet-sich-11504853.html> ✓ geprüft

L-06 WatchGuard Fireware OS: 18 Advisories, mehrere kritische Lücken ohne Anmeldung (u. a. CVE-2026-93866)

MITTEL SecurityOnline (Hersteller-PSIRT nicht direkt geprüft), 27.10.

Was ist neu: WatchGuard hat am 27.10. 18 Advisories zu Fireware OS veröffentlicht. CVE-2026-93866 ist ein Integer Overflow ohne Anmeldung im Access Portal (CVSS 9,2), der Höchstwert liegt bei 9,5. Wie viele Lücken kritisch sind, geben die Quellen unterschiedlich an (sieben oder acht). Eine Ausnutzung ist bisher nicht bekannt.

Bedeutung: Firebox-Geräte sind bei Mittelständlern und kleinen Versorgern in DACH verbreitet und stehen oft direkt am Internet. Frühere WatchGuard-Lücken stehen bereits im KEV-Katalog, Angreifer kennen diese Geräte also.

Empfehlung: Die Firmware jetzt aktualisieren und das Access Portal deaktivieren, wo es nicht gebraucht wird (CC5).

Quelle: <https://securityonline.info/cve-watchtower/cve-2026-93866/> ✓ geprüft

Empfehlungen

Nr.	Maßnahme	Bezug	Priorität	Zeitraum
M-01	Management-Interfaces von Firewalls und Edge-Geräten nur noch über einen Jump Host erreichbar machen und auf die PHP2Shell-Fixes patchen [CC2 Defensible Architecture]	L-01	HOCH	sofort
M-02	Cisco ASA/FTD aktualisieren und einen zweiten Remote-Access-Weg für Bereitschaft und Dienstleister festlegen [CC4 Secure Remote Access]	L-02	HOCH	sofort
M-03	SPS-Webserver und HMI-Zugänge inventarisieren, nicht benötigte abschalten und externe Erreichbarkeit regelmäßig prüfen [CC5 Risk-Based Vulnerability Management]	L-03	HOCH	0 bis 3 Monate

Nr.	Maßnahme	Bezug	Priorität	Zeitraum
M-04	Migration der OT-Altsysteme ohne Herstellerfix (ICONICS MC Works64/GENESIS32, NetModule) planen, bis dahin vom Remote Access trennen [CC5 Risk-Based Vulnerability Management]	L-04	MITTEL	3 bis 6 Monate
M-05	Wiederanlauf ohne zentrale Virtualisierung (vCenter) und mit Offline-Backups üben [CC1 ICS Incident Response]	L-05	MITTEL	0 bis 3 Monate

Fragen für das nächste Jour fixe

1. Welche unserer Firewalls, Router und Gateways haben eine PHP-basierte Weboberfläche, und ist deren Management-Interface aus dem Internet erreichbar?
2. Läuft unser Remote Access für Fernwartung über Cisco ASA/FTD mit sekundärer Authentifizierung, und welchen Ausweichweg haben wir, wenn das VPN ausfällt?
3. Ist der Webserver auf unseren S7-1500- und ET-200SP-CPU's aktiv, und wer darf dort Trace-Dateien importieren?
4. Welche OT-Dokumentation (Netzpläne, Geräteinventare, Firmware-Stände) liegt bei Dienstleistern, und wie ist sie dort geschützt?
5. Haben wir in diesem Quartal eine externe Prüfung auf offene HMIs und VNC-Zugänge in unseren IP-Bereichen gemacht?

Maßnahmen dieser Woche

1. PAN-OS auf die Hotfix-Stände bringen und das Management-Interface aller Firewalls nur noch über einen Jump Host erreichbar machen.
2. Herstellerlisten zu PHP2Shell (Siemens, Schneider, B&R, Belden, HMS, Wibu) mit dem Asset-Inventar abgleichen und Patches oder Workarounds umsetzen.
3. Cisco ASA/FTD auf die Fix-Version aktualisieren oder die von Cisco beschriebene Mitigation für DefaultWEBVPNGroup setzen.
4. Den Webserver auf S7-1500-/ET-200SP-CPU's abschalten, wo er nicht gebraucht wird, sonst die Ports 80/443 auf Engineering-Stationen begrenzen.
5. Mit Shodan oder Censys nach offenen HMIs, VNC und Weboberflächen in den eigenen IP-Bereichen suchen und Funde sofort schließen.
6. WatchGuard Fireware und, falls vorhanden, ICONICS GENESIS64 auf die Fix-Versionen aktualisieren.

HINWEIS ZUR QUELLENLAGE

Die Kernmeldungen habe ich an Primärquellen geprüft (Cisco, Palo Alto, CISA ICSA-26-295-14, CISA-KEV-Meldung) bzw. an heise und Bloomberg/Meduzza. Zu WatchGuard liegt nur Fachpresse vor, die Zahl der kritischen Lücken schwankt dort zwischen sieben und acht. ICSA-26-300-02 stammt aus dem Tagesbriefing und wurde nicht erneut abgerufen. Nicht aufgenommen habe ich unbestätigte Leak-Site-Einträge (Frommann Energie, Hauhinco, Ingelectus, Tema Energy) und die Veeam-Lücke CVE-2026-108142 ohne bekannte Ausnutzung. Ebenfalls nicht aufgenommen ist die Arista-VeloCloud-Zero-Day-Lücke, weil sie am 22.10. und damit vor dem Berichtszeitraum gemeldet wurde. Neue OT-bezogene Warnungen von BSI, CERT.at oder BACS (NCSC Schweiz) für die KW 44 habe ich nicht gefunden. Alle Quellenlinks wurden am 30.10.2026 automatisch aufgerufen und inhaltlich geprüft. 1 Meldung(en) ohne überprüfbare Originalquelle wurden nicht aufgenommen.